研究テーマ　顔認識の実利用に関する研究

研究者　梅村正美　東海理研株式会社　共同研究員

フェーズI

1 研究の概要

この研究では、顔認識技術をセキュリティシステムや、入退出管理などへの実利用への展開を図る。フェーズIでは、利用者の顔画像を確実に取得する方法として、顔認識技術において基盤技術となる正面顔の判定技術の確立を目指し、四方向面特徴を用いた人物によらない顔向き推定手法を開発した。また、二方向のカメラから撮影した顔画像より、各カメラの識別器出力を統合する二方向カメラ協調手法も構築し、ロッカーシステムに搭載した。

2 研究の目的

本研究では、複数方向の顔画像から抽出した四方向面特徴を用いて、人物によらない顔向き推定手法を開発した。また、複数のカメラで異なる方向から画像を取得し、各カメラの識別器出力を統合するマルチカメラ協調手法も提案する。さらに、顔向き推定手法を利用した顔向きに依らない人物識別の実験を行った。顔向き推定実験からは、推定誤差の平均が4.5°以下、分散が1現在、セキュリティシステムにおける個人認証において、ICカードの提示とパスワード入力による方法が多く採用されている。しかし、ICカードの盗難やパスワードの流出によりシステムの不正利用者が現れた場合、システムの堅牢性は崩れてしまう。事後に不正利用者を特定するため、防犯カメラを設置する場合でも、利用者の顔を必ずしも撮影できるわけではない。

そこで、本研究では利用者の顔を確実に撮影するカメラを搭載したセキュリティシステムの構築を目的とする。本システムでは、ICカードの提示とパスワードの入力による個人認証を行い、次いで利用者の正面顔を取得し、保存する仕組みになっている。顔画像による人物認識は行わないが、正面顔を取得できなければシステムは動作せず、不正利用を防止できると考えられる。

本人照合のためのバイオメトリクス情報として、顔認識の研究が盛んに行われており、入退室・施錠管理への応用なども行われている。今回のシステムでは、従来のID、パスワードのセキュリティシステムに、事後確認に必要な顔画像取得を組み込むことを目的とする。

本稿では、本システムに用いる正面顔判定手法について述べ、顔の向きに対する実験について考察する。正面顔検出には4方向面特徴を用いる。4方向面特徴は主に文字認識の分野において有用性が示され、人物認識、顔方向識別にも応用されている。本システムは不特定多数の利用者を想定しており、平均顔辞書を使用することにより、これに対応する。平均顔辞書の作成には、年代・性別が均等に含まれているデータを用いることにより、年齢・性別を問わず検出を行うことが可能となる。正面顔検出実験において、平均顔辞書の作成時と異なる環境下で撮影したデータに対し正しく正面顔を検出できることを示し、汎用的なセキュリティシステムの運用に、本手法が有効であることを示す。

3 実施内容

3.1 システムの概要

本システムは、ID・パスワード認証型セキュリティシステムにカメラを搭載し、利用者の正面顔を確実に撮影するものである。今回は構成例として、貴重品ロッカーに顔撮影システムを組み込んだ。図1にシステムの全体像を示す。中央にインタフェースがあり、その周囲に各利用者のロッカーがある。図2にインタフェース部の拡大図を示す。ICカードリーダー、利用者を撮影するカメラ、パスワード入力と利用者の顔画像を表示するタッチセンサー式液晶ディスプレイで構成されている。

図 1　システムの外観

図 2　インタフェース部分

このシステムの利用手順は以下のようになる。

1) IC カードを提示する。
2) パスワードを入力する。
3) 液晶ディスプレイの表示に合わせ、顔を向ける。
4) ロッカーが開錠される。

システムはまず利用者に IC カードの提示とパスワードの入力を求める。これは従来のセキュリティシステムと同様の操作であり、この操作で個人認証を完了する。本システムでは、これに加えて利用者に正面顔の提示を要求する。このとき、カメラからの入力画像が液晶ディスプレイに表示される。利用者は液晶ディスプレイに自分の顔が写るように移動する。後述の正面顔検出手法により入力画像中に正面顔が検出されると、本システムは利用者の正面顔画像を保存し、利用者のロッカーを開錠する。つまり、利用者の正面顔が検出されない限り開錠しないので、確実に利用者の顔画像を取得できることになる。

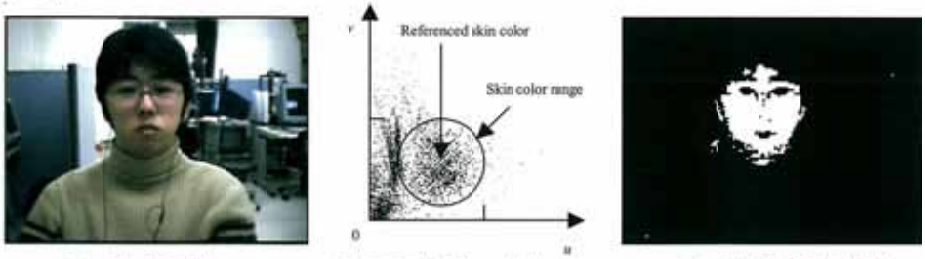
取得した顔画像と利用日時などの情報は、ログとして保存される。不正利用があった場合、事後にログを検索し、保存された顔画像を見ることで、不正利用者を特定することができる。

3.2 正面顔検出手法

本システムにおける正面顔の検出手法の流れを述べる。入力画像から肌色領域を抽出し、肌色領域内から顔候補領域を抽出する。4 方向面特徴を用いて、候補領域周辺を探索し、類似度計算により正面顔を検出する。

3.2.1 色情報を用いた肌色領域抽出

顔の検出に色情報を用いる方法は広く使われているが、今回は背景や照明環境に比較的ロバストな肌色基準値法を用いる。まず、入力画像を CIE-L*u*v*表色系に変換し、u*, v*値の 2 次元ヒストグラムを作成する。図 3(b)は図 3(a)の u*, v*値の分布を示している。あらかじめ定めておいた肌色有効範囲内で、最も画素数の多い値を肌色基準 u*, v*値とする。肌色有効範囲は事前にカメラ特性や照明条件に応じた値を設定しておく。次に肌色基準 u*, v*座標値と入力画像の各画素との距離を求め、判別分析法を用いて 2 値化する。肌色検出例を図 3(c)に示す。この領域に雑音除去、穴埋めを施し、面積が最大となる領域を選定する。ここで得られた肌色領域を R_1 とする。



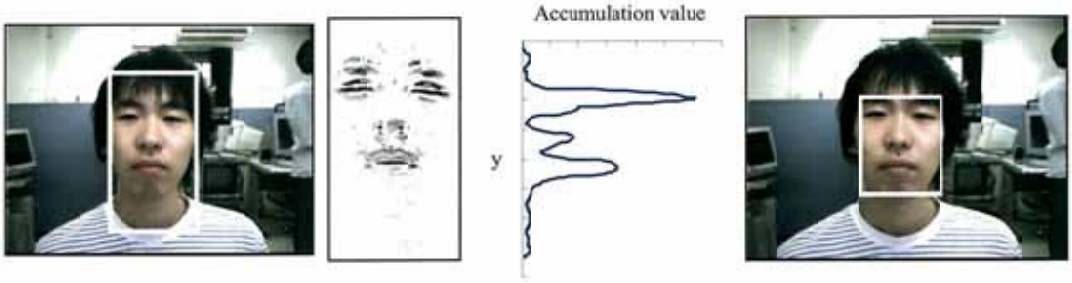
(a) 入力画像　(b) UV カラー分布　(c) 肌色抽出結果

図 3 肌色抽出

3.2.2 水平成分を用いた顔候補領域抽出

肌色領域 R_1 は、図 4(a)のように利用者の服装によって顔だけでなく首も含まれる。そこで、肌色領域から顔候補領域を絞り込む。

肌色領域内の水平成分を、横方向に射影した累積ヒストグラムを作成する。このヒストグラムを十分に平滑化すると、目や眉付近をピークとするヒストグラムが得られる。図 4(a)の肌色領域内の水平パターンを図 4(b)に、ヒストグラムを図 4(c)に示す。ピーク値から固定値 α 上の位置を、顔候補領域の上端とする。肌色領域の横幅を顔候補領域の横幅とする。固定の縦横比で顔候補領域 R_2 を決定する。求めた顔候補領域を図 4(d)の矩形で示す。領域の縦横比を 1 : 1.1 とする。この比率は予備実験により得られた値である。

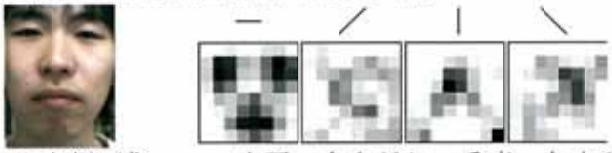


(a) 肌色領域　(b) 水平成分　(c) ヒストグラム　(d) 顔候補領域検出結果

図 4 顔候補領域検出

3.2.3 ４方向面特徴

４方向面特徴は文字認識、人物認識など、パターン認識の分野で広く使われている特徴量である。４方向面特徴の作成手順を以下に述べる。入力画像から、方向検出フィルタにより、水平・垂直・右上がり・右下がりの各方向の４方向面を作成する。これら４面をそれぞれ正規化・ぼかし処理・低解像度化し、各方向面の画素の濃淡値を特徴量とする。予備実験により特徴面の解像度は 8×8 とした。図 5 に４方向面特徴の例を示す。



入力顔画像　水平　右上がり　垂直　左上がり

図 5　４方向面特徴

3.2.4 顔領域探索と正面顔検出

3.2.2 節で述べた顔候補領域 R_2 では、ヒストグラムのピークが得られない場合があり、図 6(a)のように検出位置がずれてしまう。そこで、テンプレートマッチングにより顔領域を補正する。

得られた顔候補領域 R_2 周辺を、4 章で述べる平均顔辞書 T を用いて、テンプレートマッチングを行う。テンプレートマッチングには（1）式の類似度 E を用いる。

$$E = \sqrt{\frac{\sum_n I_n T_n}{\sum_n (I_n)^2 \sum_n (T_n)^2}} \qquad (1)$$

ここで I は入力特徴、T は平均顔辞書、n は特徴次元数を表している。類似度が最大となる領域を顔領域 R_3 とする。テンプレートマッチングにより正しい位置に修正された例を図 6(b)に示す。

正面顔検出には、ある閾値 Th 以上の類似度 E が得られた場合に、正面顔を取得できたこととする。類似度閾値 Th は固定値であり。多方向顔画像データベースを用いた予備実験により事前に求める。また、利用者の顔のぶれや、誤検出を防ぐため、複数フレーム連続で顔画像が取得できる場合に、顔画像を受理することとする。ここでの連続フレーム数 k は利用者の負担にならない程度に調整する。

(a) 顔領域検出失敗　　(b) 顔領域補正

図 6　顔領域の補正例

3.3 4 方向面特徴による平均顔辞書

本手法では正面顔判定に平均顔特徴を用いる。一般に言われる平均顔とは顔領域内の特徴点を手動で設定し、各特徴点を平均し作成する。本手法では多方向顔画像データベースの正面顔画像を用い、多人数の顔画像から得られた 4 方向面特徴を平均することにより正面顔の特徴を取得する。これを一般に言われる平均顔と区別するため、平均顔辞書とよぶ。

3.3.1 辞書作成用データ

辞書作成用画像として、多方向顔画像データベースの正面顔画像を用いた。このデータベースは 15 歳～64 歳迄を年代別･性別を均等な人数に振分け、計 300 名を収集したものである。図 7 に例を示す。性別・年齢が多岐にわたる多数の正面顔画像を用いることにより、少数の顔画像から作る場合に比べ、より汎用的な辞書の作成が可能となる。

図 7　多方向顔画像データベースでの正面顔例

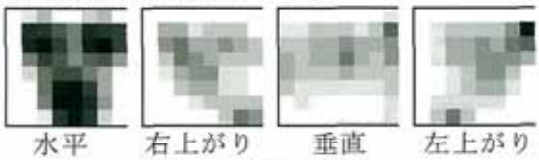
3.3.2 平均顔辞書の作成

顔候補領域 R_2 を単純に用いただけでは、顔領域の位置がずれてしまうことは、3.4 節で述べた。位置のずれた領域より平均顔辞書を作成することは適切でない。そこで次のような手順で平均顔辞書を作成する。

まず、正面顔画像から 3.2 節で説明した顔候補領域 R_2 を用いて、4 方向面特徴を抽出し、300 人分の平均を算出する。これを平均顔候補テンプレート T'とする。

次に、顔領域を補正し、平均顔を再度作成する。顔候補領域 R_2 の周辺を、正面顔候補テンプレート T'でテンプレートマッチングをする。類似度が最大となる領域を顔領域 R_3'とする。顔領域 R_3'の 4 方向面特徴を平均し、平均顔辞書 T を作成する。

上記手法により作成した平均顔辞書を図 8 に示す。



水平　右上がり　垂直　左上がり

図 8　平均顔辞書

4 結果

平均顔辞書を用いた正面顔判定の実験を行った。まず、本システムでの正面顔を定義する。正面顔判定に必要な閾値の設定と、別環境下での実験を述べる。また一般的な平均顔との比較実験についても述べる。

4.1 正面顔の定義

ここで、今回適用する正面顔の定義を示す。正面顔は両眉、両目、鼻、口の顔パーツが欠けることなく画面内に収まっている顔画像とする。これを顔画像データベースに適用すると、図

9(a)のような 0°から 15°は正面顔となる。図 9(c)のように 45°以降横を向いた画像は顔パーツのいくつかが欠けてしまうので、正面顔ではないとする。図 9(b)のような 30°付近は、個人差により顔パーツが欠ける画像とそうでない画像とがあるので、どちらともいえない場合として扱う。

(a) 正面顔　　(b) 中間　　(c) 非正面顔

図 9　正面顔の定義

4.2 平均顔との比較

一般的に平均顔とは、顔パーツの特徴点を手動で合わせ、アフィン変換等により画像を平均したものを指す。提案手法との比較のため、平均顔から作成した 4 方向面特徴を辞書とした正面顔判定の実験を同時に行った。今回用いた平均顔は、多方向顔画像データベースの 300 人分の正面顔画像を用いて作成した。作成した平均顔を図 10 に示す。この画像の作成には FaceFit および平均顔作成ツールを用いた。

図 10　300 人分から作成した平均顔

4.3 HOIP 顔画像データベースに対する実験

多方向顔画像データベースを対象に正面顔検出実験を行い、最適な類似度閾値を求める。入力画像として、300 人の多方向顔画像を使用した。それぞれ正面に対して左右に 0°から 75°まで 15°刻みの画像を用意し、1 人あたり各方向 1 枚ずつ、計 3,300 枚を使用した。

結果を図 11 に示す。類似度閾値 Th を 0.7 から 0.9 まで推移させている。提案手法は、平均顔から作成した 4 方向面特徴よりもよい結果を得た。平均顔から抽出した特徴は、個人のばらつきとなる分散を十分表していない。それに対し、本手法の 4 方向面平均顔では、特徴量の分散により個人の差を吸収すると考えられるため、よい結果を得たと推測される。提案手法においては、類似度閾値 Th=0.8 であるときに最もよい結果が得られた。

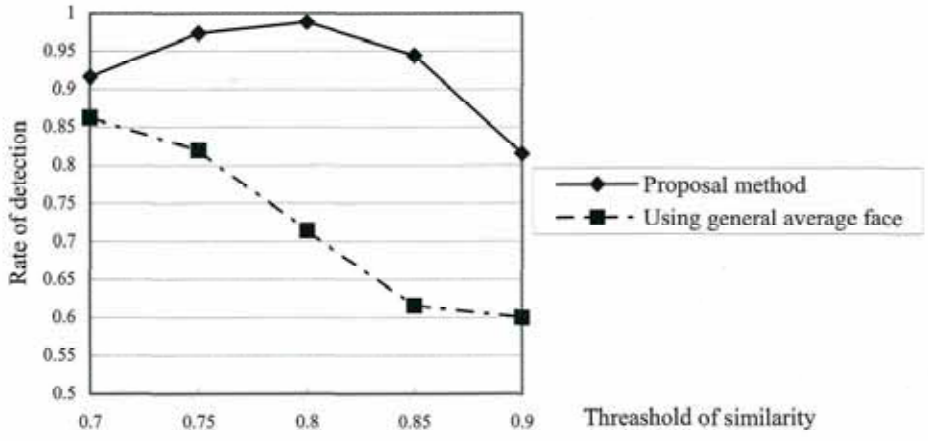


図 11　HOIP データベースに対する正面顔判定結果

4.4 実利用環境下での実験

顔画像データベースから作成した 4 方向面特徴平均顔および、先に求めた類似度閾値を用い

て、正面顔判定実験を行った。実験データの撮影は、辞書画像撮影時とは異なるカメラ・場所・時間で行った。また背景は実利用環境を想定し、複雑背景とした。被験者は 17 人で、カメラに対し 0°から 75°まで 15°刻みの方向を向き、それぞれ秒間 3 フレームで 30 秒間撮影した。実験データの画像例を図 12 に示す。

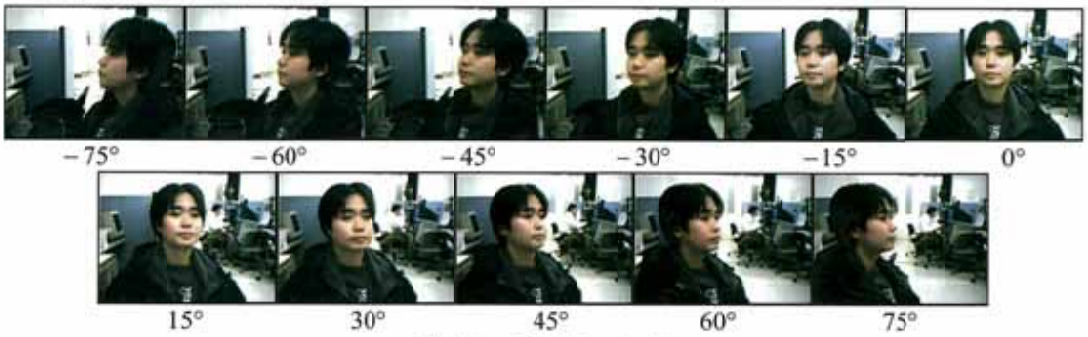


図 12　実験データ例

正面顔検出のパラメータとして、類似度閾値 Th=0.8、連続フレーム数 k=3 とした。実験結果を表 1 に示す。全ての被験者において、正面顔を正しく検出し、正面でない顔を除外することができた。このことから顔画像データベースから作成した正面顔辞書と、同データベース内の多方向の顔画像から求めたパラメータが、異なる環境下においても有効であることが示された。

表 1　別環境下での正面顔判定結果

Direction of face (degree)	0	15	30	45	60	75
Detection (number of person)	17	17	7	0	0	0
Rejection (number of person)	0	0	10	17	17	17

4.5 連続撮影時の類似度変化

図 13 のグラフでの細線は、秒間 10 フレームで正面顔を連続して撮影した場合の類似度の推移を表している。利用者の瞬きなどの変動により、瞬間的に類似度が低下する。顔のぶれや、誤検出を防ぐため、複数フレームの類似度を使用するが、ここでメディアン値を正面顔判定に利用すると、安定した検出が可能になる。図 13 の太線は、9 フレームを用いたメディアン値を表している。スパイク状の類似度低下に影響されずに、安定した値を保っていることがわかる。

以上、正面顔検出において、辞書作成とは異なる環境下であっても、良好な結果を得た。このことから、1 つの 4 方向面特徴の平均顔辞書により、不特定の人物、異なる環境に対し有効であることが確認された。

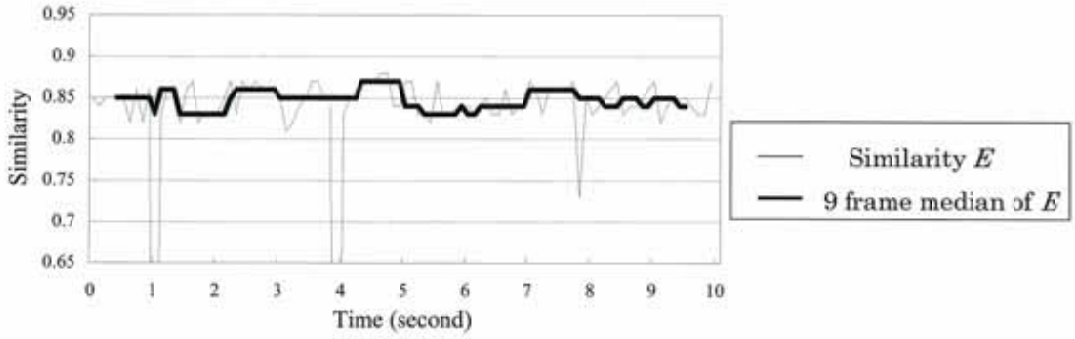


図 13　類似度の推移

フェーズ II

1 研究の概要

フェーズ II ではフェーズ I での研究成果をもとに、製品化を目的とした応用展開を図る。二方向からの顔画像取得による入退出管理システムの構築をめざす「二方向からの顔画像、身体画像による個人照合システムの開発」と、各種セキュリティシステムをネットワーク化し、顔認識を一元的に管理する「グループ階層ネットワークを使用した本人照合機能の研究」を実施

した。

2 二方向からの顔画像、身体画像による個人照合システムの開発

2.1 概要

本研究内容は二方向からの顔画像、身体画像による個人照合により入退室制限を行い、不正入退室を防止するシステムの研究を実施した。

本研究の目的は、従来の入退室システムでは、IC カードを本人以外が使用しても本人であるかどうかを識別できない為、本人以外になりすます事が可能である。又、扉が開いている間は、IC カードを提示した本人以外の複数人の不正入退室が可能で、IC カード提示者以外の不正入退室が可能となり、何の為に入退室管理を行っているか意味がなくなってしまうという問題があります。そこで今回の研究テーマである「二方向からの顔画像、身体画像による個人照合システムの開発」を実施することで、IC カード、顔認証、入退室する人物が 1 名であることの 3 つの条件がそろわないと入退室できないシステムにすることで問題を解決する。

本研究用で図 14 の部屋への入退室のモデルを試験的に製作し、試験、検証を実施した。図 15 に示すように、顔認証、身体画像、IC カードリーダー、履歴管理システムをそれぞれ独立することで、システムの組み合わせを可能にした。各システム間はイーサネットで接続し、TCP/IP、FTP 等のプロトコルで通信を行い、主制御システムがなくても動作可能なシステムとした。顔画像検出カメラを 2 基、動体検出カメラを 1 基の画像データをビデオスイッチャー経由で、顔認識システムに入力した。顔認識システムに入ったカメラ 3 台の画像をそのまま動体検出システムに送り、動体を検出する。情報はイーサネット経由で履歴管理システムに送られ履歴保存される。IC カードリーダーは読み取った IC カードのデータをコントローラ、イーサネットを経由して履歴管理システムに送られる。顔照合ＯＫ、動体 1 名のフラグを受け取り電気錠を開錠する。

システムは、図 16，図 17 に示すように、IC カードを使用したのが本人であるかどうか IC カードを使用した人の顔画像データとデータベース上の IC カードの固有番号に登録されている顔画像データを照合し、本人かどうかの特定を行い、入退室扉の特定エリア内に複数人（2 名以上）の動きを検出しなかった場合電気錠を開錠して、入退室を許可する。又、扉が開いた後も身体画像をモニターすることで、不正に入退室する人を監視する。入退室した情報は、入退室時間、カード番号、顔画像を履歴として保存し、不正発生時の状況を確認できる。

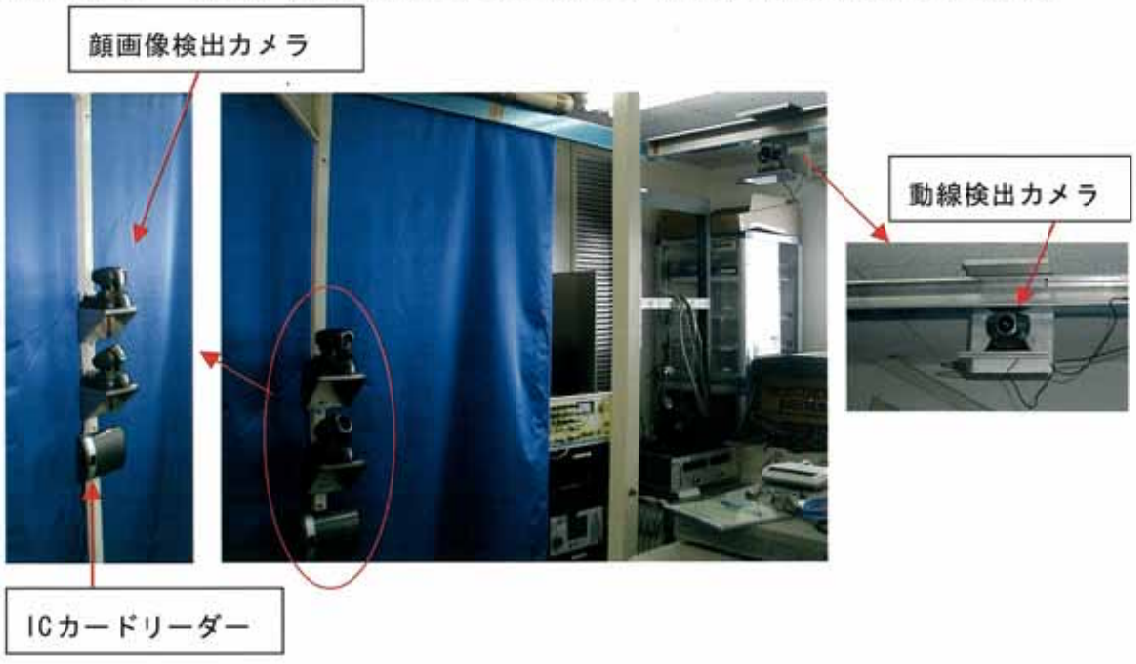


図 14　入退室モデルの試験機

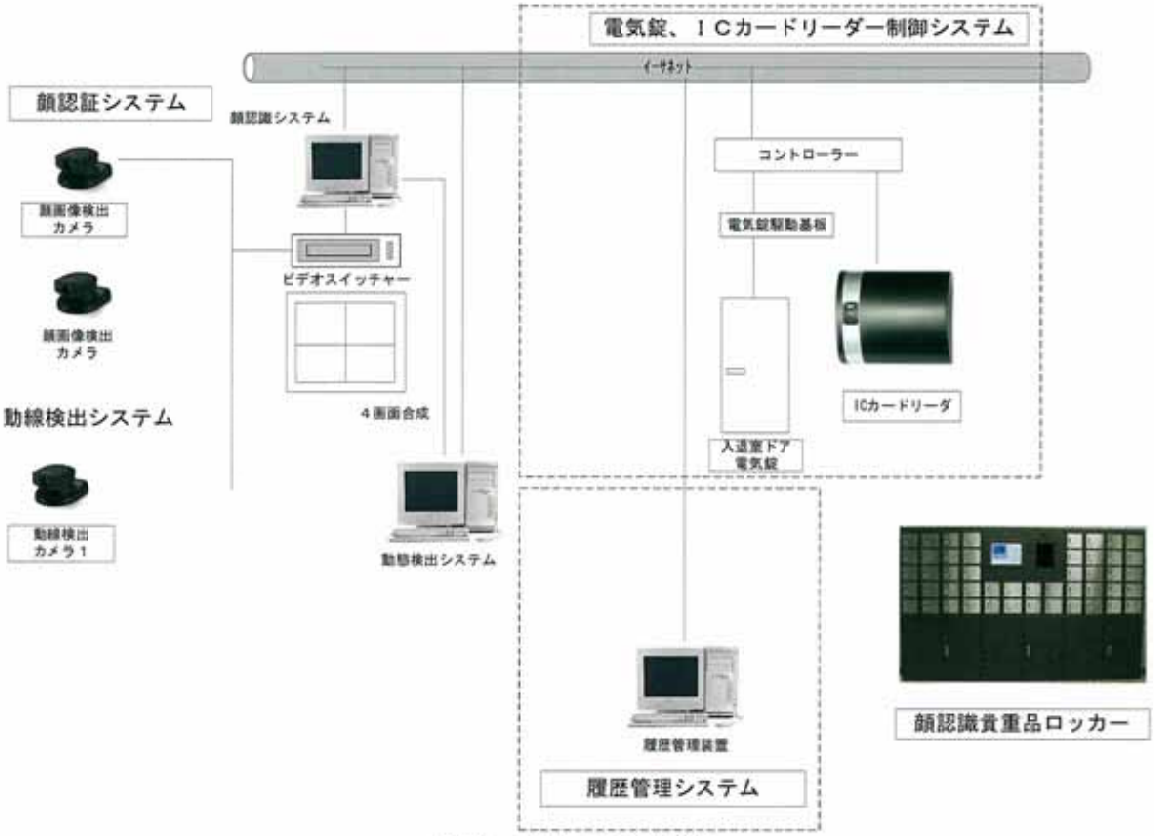


図 15　システム構成図

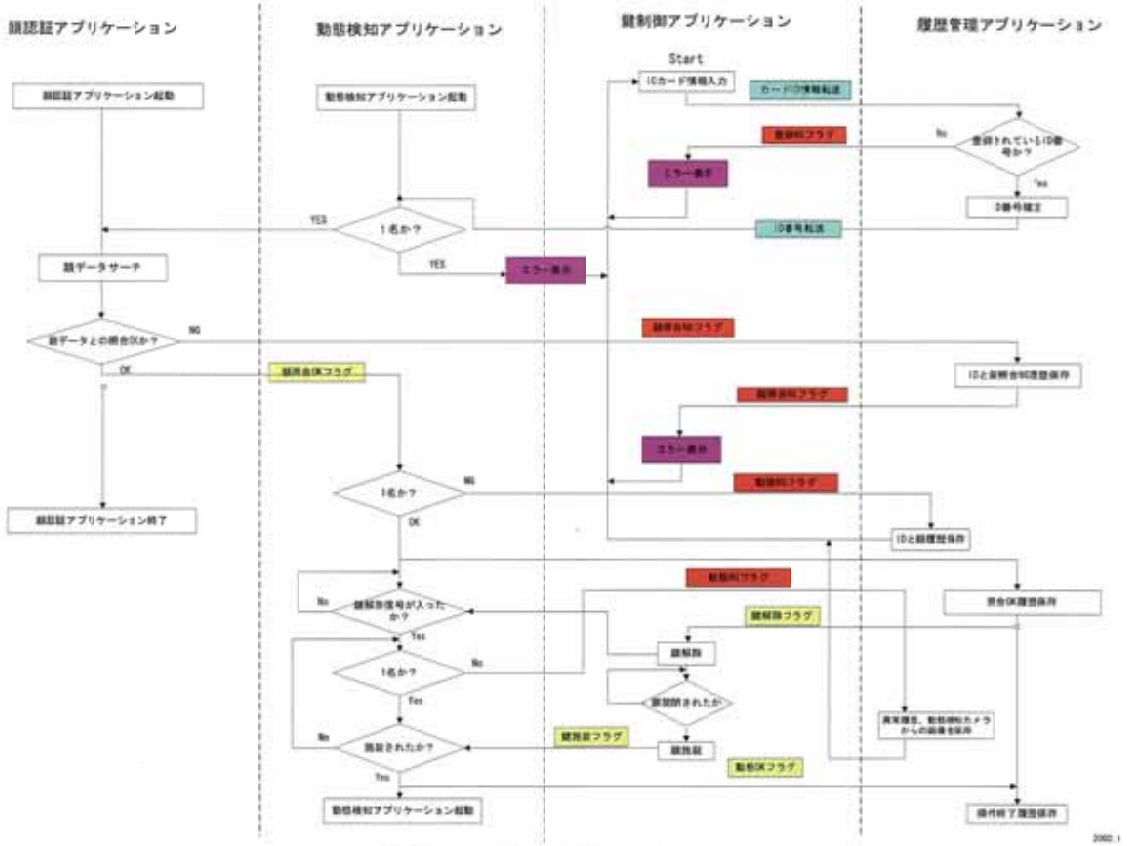


図 16　フローチャート

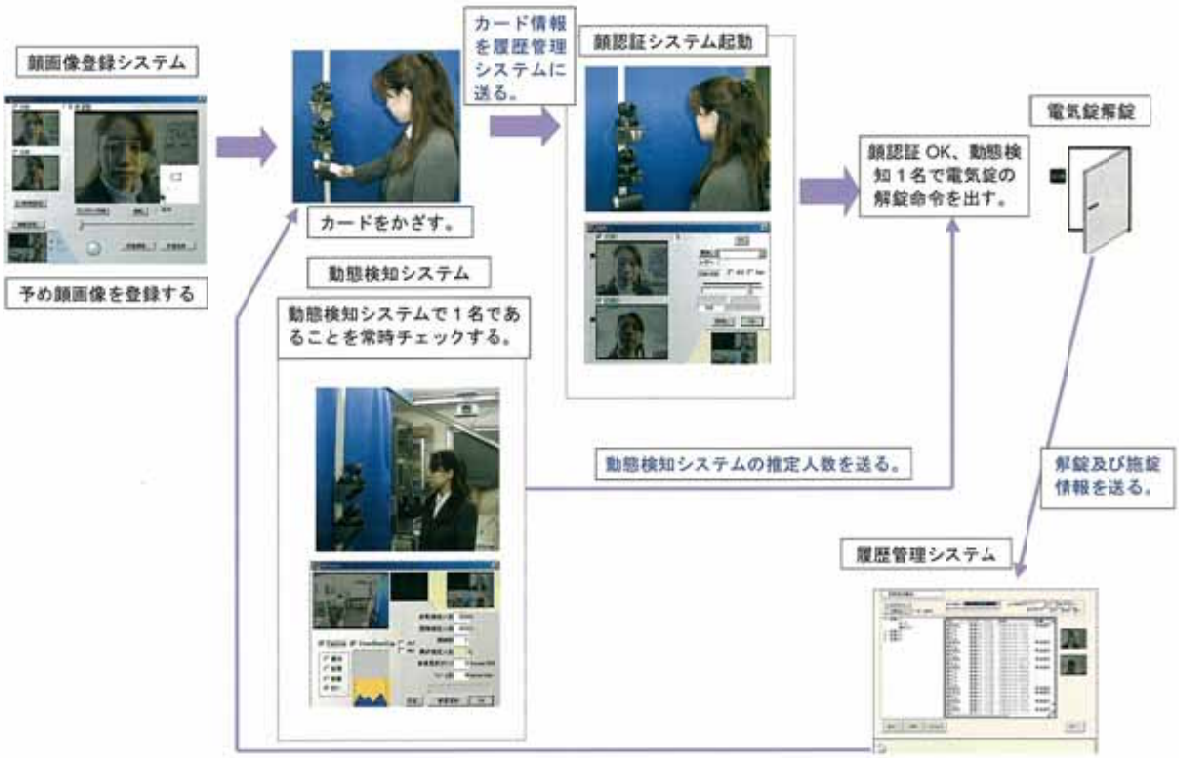


図 17　動作フローチャート

2.2 実施内容

１．顔認証アプリケーション：

開発当初は、顔の正面顔と右又は左の顔画像で認識する計画だったが認識精度が向上しなかった為、正面顔と正面斜め下からの画像を取り込み認証処理を行った。又顔画像登録時に複数枚の顔画像を辞書化し複数枚での認識を行うようにした事で、照合精度の向上と本人排他率の低減を行った。本人照合率は、環境及び閾値に影響されますが、50～60%の照合は得られた。

当初は、顔認証アプリケーション、動体検知アプリケーションを１台の専用機で情報処理する予定だったが、顔認証アプリケーションの動作が１台の専用機での処理能力を越え、取得フレーム数が減少した為、顔認証アプリケーションと動体検知アプリケーションの動作環境を変え各１台の専用機を使用し処理を行うようにした。

２．動体検知アプリケーション：

開発当初は、扉の外内の２箇所に設置し入室退室の動体を検出する計画だったが、２カメラでの動体の切り替えが出来なかった為、１カメラで動体検出を行った。又、背景差分の手法を用いていることもあり、扉の開閉で輝度の変化が顕著に発生し人物の動きが検出できない問題が発生した。この問題の解決として扉は固定されている条件で、扉部分をマスクし差分データが入れない手法で解決した。問題点として蛍光灯のちらつきが背景差分のデータとして入ってしまいちらつきが大きい場合人物の差がはっきりしない状況が発生したが、現在人数判定パラメータの設定で解決した。

３．ICカードリーダー：

非接触ICカードを使用し入退室を制限する。非接触ICカードはSONY製のカードを使用し、カード固有のユニークな番号（IDm　１６桁）を読み取りデータを照合し入退室が許可される。電気錠の制御もカードリーダで行い、通信手法としてTCP/IP（10Base-T）を使用し高速にデータのアップ及びダウンロードが可能である。読み取ったICカードデータはカードリーダー内部にメモリすると共に顔照合、履歴管理アプリケーションに送られ、それぞれシステムを稼動する。

カードリーダーに蓄積される履歴データは、Web Saver を搭載しているため、インターネットエクスプローラーで閲覧可能である。又履歴情報、ID 情報、機器の初期設定を FTP 経由でインターフェースされるので、スタンドアローンは勿論のこと顔認証、動体検知アプリケーシ

ョンとの動作リンクも容易に行え、他機器とのリンクも可能である。

2.3 結果

2.3.1 登録アプリケーション

入退室管理システムの顔照合を行うためのアプリケーションであり、図 18 に示す。顔照合を行うための顔データは複数枚登録し、顔照合を行う際には複数枚を参照する。顔データと顔照合画像は、同じ環境条件で行った方が認識率が高いため、このアプリケーションは、顔認証システムに搭載している。

顔データ辞書については図 19 のように、撮影した顔データを表示し、目、鼻、口の部分を切り出す。目、鼻、口を表示していない顔画像は、使用しても照合のデータにはならない為、予め削除する。

図 18 登録アプリケーション

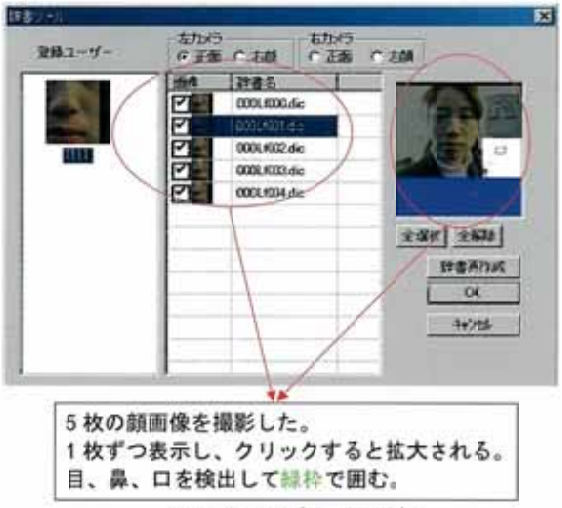


図 19 顔データ辞書

2.3.2 顔照合アプリケーション

顔照合アプリケーションを図 20 に示す。カメラ映像を取り込み目、鼻、口を検出し登録辞書と比較し本人照合を行う。設定された制限時間内で認証 Hit 回数（設定されたしきい値を上回った連続した回数）に達すれば照合結果として OK を返す。

図 20 顔照合アプリケーション

図 21 に示すように、「0003」で顔データ登録をした人物を認証した場合に、しきい値を 0.7 程度にするとＯＫの検出をする。しきい値を 0.7 以上にするとＮＧの検出する回数が増える。条件は、認証Ｈｉｔ3 回で検出している。

図 22 は、「0003」で顔データを登録していない人物を認証した場合である。ＮＧを出すしきい値は 0.7 程度である。条件により精度の向上は可能となる。人物の後ろ写っている蛍光灯の影響も少なくないと思われる。又、顔画像の大きさ等により影響される。

図 21 顔照合例

図 22 蛍光灯の影響

2.3.3 動体アプリケーション

動体アプリケーションを図 23 に示す。これは、視体積交差法を用いて動体の検知を行う。

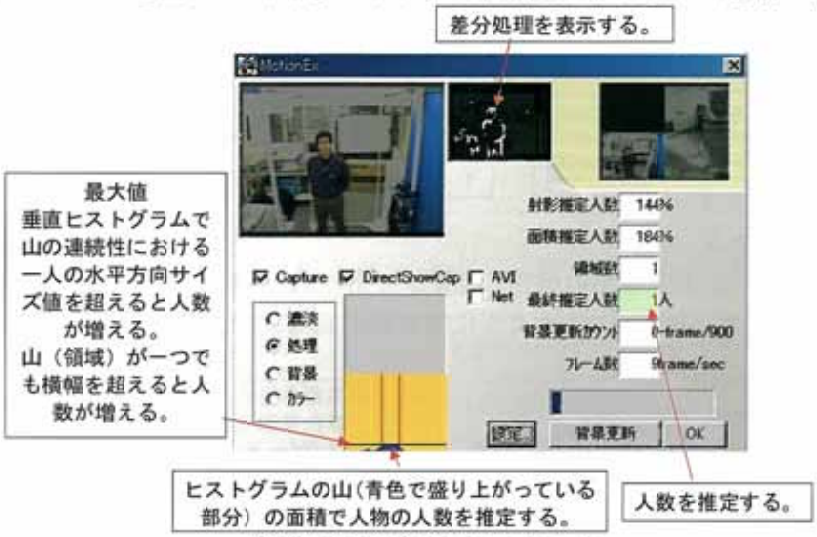


図 23 動体アプリケーション

実際に 2 名入った時の実験データを図 24 に示す。しきい値の最小、最大を近似値、面積を 200 程度に設定した場合に 1 名、2 名の切り分けができる。但し、設置環境により精度が左右されるので、設置場所で調整が必要になる。

このときのしきい値は図 25 のように、調整可能である。

図 24 実験データ例

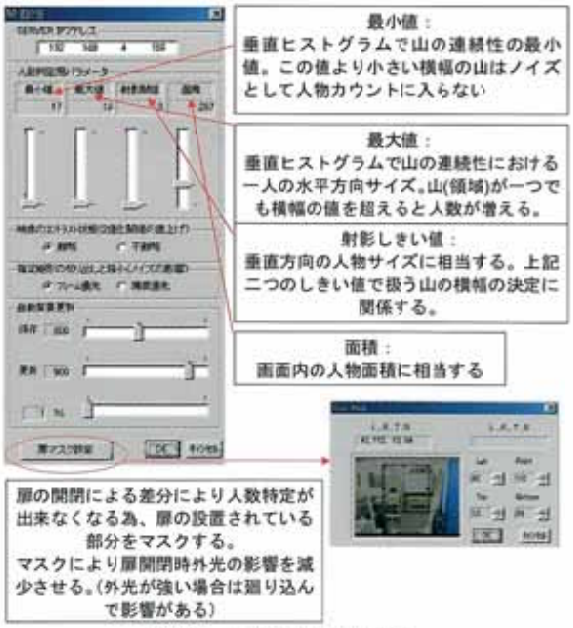


図 25 しきい値の調整

2.3.4 IC カードリーダー

IC カードリーダーの外観を図 26、その仕様を表 2 に示す。非接触 IC カードを使用し入退室を制限する。非接触 IC カードは SONY 製のカードを使用し、カード固有のユニークな番号（IDm16 桁）を読み取りデータを照合し入退室が許可される。

電気錠の制御もカードリーダで行い、通信手法として TCP/IP（10Base-T）を使用し高速にデータのアップ及びダウンロードが可能である。

読み取った IC カードデータはカードリーダー内部にメモリすると共に履歴管理パソコンに送る。カードリーダーに Web Saver を搭載しているので、インターネットエクスプローラーで閲覧可能である。又履歴情報、ID 情報、初期設定は、FTP 経由でインターフェースされる。

図 26 IC カードリーダー外観

表 2 IC カードリーダー仕様

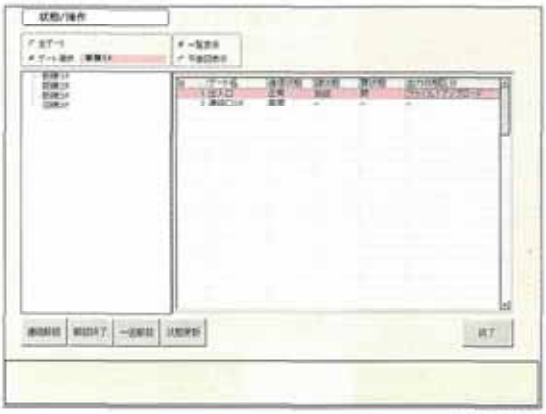
外形寸法	172（W）×142（H）×44（D）
非接触カード	フェリカ（ISO14443 Type C）
読み取り距離	Max　１０ｃｍ以下（使用環境により異なる）
表示	LED3 ヶ（OK ランプ（緑）、解錠ランプ（黄）、エラーランプ（赤））
インターフェース	TCP/IP(10Base-T)

2.3.5 履歴管理システム

図 27 に示すように入退室履歴の保存、閲覧が可能である。各利用状況をデータベースに保存し閲覧が出来る。また、図 28 に示すように電気錠の施解錠は遠隔で操作できる。

履歴の検索条件を入力する。
ゲート、または個人を選択する。
①「エリア/ゲート」、または「所属/個人」を選択する。
②ツリーにて対象ゲート、または個人を選択する。
（「個人一覧表示」を選択した場合、個人一覧から個人を選択する。）
出力状態区分を選択する。
（入室、退室、不正アクセス、遠隔操作 1 回解錠、連続解錠、火報 ON、外部入力 ON、時計修正、タイマー解錠、入室禁止時間開始、ID 入室許可開始、オペレーション履歴）

図 27 履歴管理



「連続解錠」ボタン
　選択したゲートを強制解錠する。「解錠終了」を送信するまで、解錠し続ける。
「解錠終了」ボタン
　選択したゲートが「連続解錠」にて解錠している場合、強制解錠を取り消す。
「一回解錠」ボタン
　選択したゲートを設定時間だけ強制解錠する。
「状態更新」ボタン
　選択したゲートの通信状態・鍵状態・扉状態を表示する。

図 28 電気錠の施解錠

2.4 小括

顔認識、動線検出、IC カードリーダー（鍵制御部含む）、履歴管理システムの各アプリケーションをモジュールとして開発し、それぞれ個々のアプリケーションとして動作する。各アプリケーション間は、FTP 及びパケット通信で情報のインターフェースを行う。各アプリケーシ

ョンが独立して動作するので、顔認識、動線検知、ICカードリーダー、履歴管理システムをそれぞれ組み合わせることで、例えば顔認識とICカードリーダー、ICカードリーダー単独使用が可能で、市場のニーズにマッチングすると考えられる。

現在ICカード＋顔認識＋動体検知で入退室管理を行う商品は存在しない為、市場への参入は十分に可能であると判断する。又、顔認識の精度が100%でなくてもカードをキーとして顔照合を副媒体と考えれば100%の照合は必要ないと判断できるため、早期の市場投入を目指す。顔の切り出しに関しては、環境による認識精度が落ちない為、フェーズIに実施した「貴重品ロッカー」にそのまま搭載可能だと考えられる。

3 グループ階層ネットワークを使用した本人照合機能の研究

3.1 概要

3.1.1 研究の概要

本研究は本人照合により、アクセスした利用者に応じたグループ階層によるアクセス権限をネットワークを経由して付加し、システム上に設置されるサーバ及びクライアントのフォルダ（情報）へのアクセス権限、ネットワーク書庫、ネットワークデスク等のセキュリティ機器へのアクセスを制限することで、不正アクセス、不正操作を防止するシステムを研究実施した。

3.1.2 研究の目的

本研究の目的は、ICカード、暗証番号等を併用し本人照合を行うと、クライアントパソコンへのログイン、ログインと同時にICカードに設定されるグループ階層のアクセス権限を付加するシステムである。権限を付加されると、同システム上にネットワーク接続されるネットワーク書庫、ネットワークデスク等のアクセス権限を与えられる。例えば、部門毎に横割を行い、役職毎に縦割りを行うと、マトリックス状に権限付加パターンが配置できる。他部署の者は書庫を開錠不可にする事、デスクにおいては、本人若しくは上司しか開錠できない等の設定が可能となり、権限が細分化できる。

又、パソコンにICカードを使用してログインしていなければ機器の操作ができない等ネットワーク機器を鍵として利用することも可能で、物、財産、情報、人の管理までのトータルセキュリティシステムの構築が可能である。

3.1.3 システムの特徴

1) 全ての情報がサーバーに集約し、ログイン、開錠権限を設定することができる。例えば勤怠タイムレコーダーから入る出勤情報により、ネットワークデスク、ネットワーク書庫、更衣ロッカーの使用権限を与えることができる。出勤してなければ機器の操作、ログインする事ができないセキュリティの高いシステムを構築することができる。

2) 全ての機器の操作を1枚のICカード（社員証）にすることで1枚のカードで出勤、退勤の管理から機器の操作権限まで、将来的には、電子マネーの利用まで発展するシステムである。

3) ICカードに予め付加された階層ごとの権限が付加され、ネットワークデスク、ネットワーク書庫、更衣ロッカーへのアクセスを制限するとともにログイン時のサーバーへのアクセスを制限しシステム全体の不正アクセスを防止する。

4) 勤怠タイムレコーダー、ネットワークデスク、ネットワーク書庫、更衣ロッカー単独でシステム構成でき、ユーザーの要望に応じたシステム構築が可能で幅広い対応が可能である。

5) 勤怠履歴、各機器へのアクセス、サーバーフォルダーへのアクセス履歴を全てサーバーに集約することができ、履歴調査による不正アクセスの発生を追跡調査することが可能である。

3.2 実施内容

3.2.1 ICカードでパソコンへのログイン

パソコンのログイン画面が表示されてから、ICカードをカードリーダー上に提示すると、ICカードのID番号を認識し、登録されているIDであれば、暗証番号入力後ログイン権限を与える。同時にサーバーへのアクセス権限を付加し、パソコンから離れる場合にICカードをカードリーダーから外すとパソコンがロックされ操作不能状態になる。再度ICカードをカードリーダ

ーに置くとログインできる。システム構成でネットワークデスクと連動すると、ログイン時にデスクのロックを開錠し、ログオフ時又はパソコンの電源を切る場合に施錠を行う事が可能である。ログインしたパソコン上から遠隔でネットワーク書庫の開錠指示が可能である。

3.2.2 ネットワークデスク

机の引出しの電気錠施開錠を行う。従来、引出しは鍵で管理されているが、鍵を使用せず電気錠で鍵の施解錠を行う。引出しの方袖を1ブロックとし、ソレノイドで開錠を行い、ソレノイドにはソレノイド動作をモニターするセンサーを取り付け動作の確実性を高めている。又各引出しにもセンサーを配置し引き出し状態をモニターし、施錠時1つでも引出しが開かれていたらエラーを出力（ブザー、モニター上）する。

上記の構成により、引出しが両袖に付いたタイプ、片方にしか付いていないタイプ、さまざまな引出しの構成に対応し、新規ではもちろん、既存のデスクにも取り付けられるように開発を実施した。

3.2.3 ネットワーク書庫

開錠権限のある ID 番号がアクセスされたときロックを開錠し、権限設定されていない扉は開錠することができない。各扉、各引出しに電気錠を配置し、開錠指示に従い動作する。電気錠には動作確認用のセンサーを取り付け動作の安定化を行っています。各扉、引出しには開センサーを配置し閉め忘れ、こじ開けが発生した場合は、エラーを出力する。書庫の形状も扉タイプ、引出しタイプ、引き違い戸タイプがあり配置構成もさまざまで、どのような配置でも対応できるように書庫の上下1組を1ユニットとし、ユニットの増設で対応できるようにシステムを構成し、拡張性を考慮したシステムの開発を実施した。

3.3 結果

3.3.1 システム構成

図 29 にシステム構成図を示す。サーバを基点に勤怠タイムレコーダー、ネットワーク書庫、ネットワークデスク、更衣ロッカーを同一ネットワーク上に配置し、勤怠情報で出勤にならないとパソコンへのログインができない、パソコンにログインしないとネットワーク書庫、ネットワークデスクにアクセスできないシステムとした。システム運用のフローを図 30 に示す。

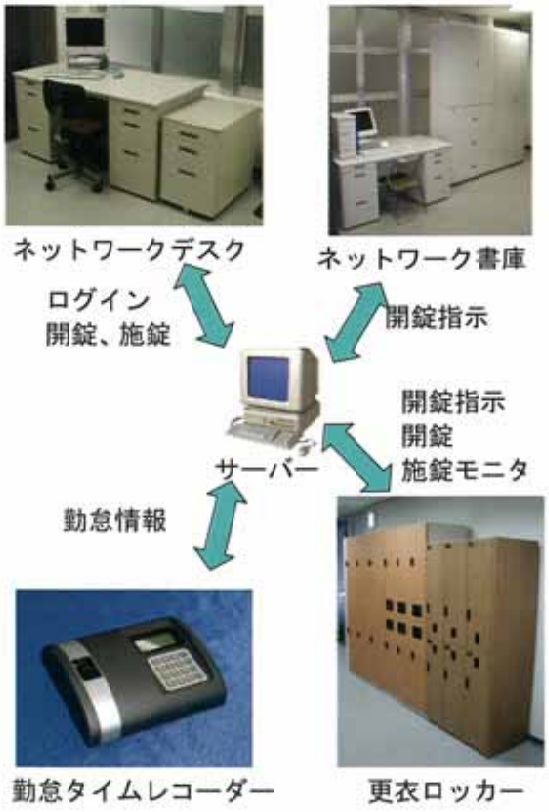


図 29 システム構成

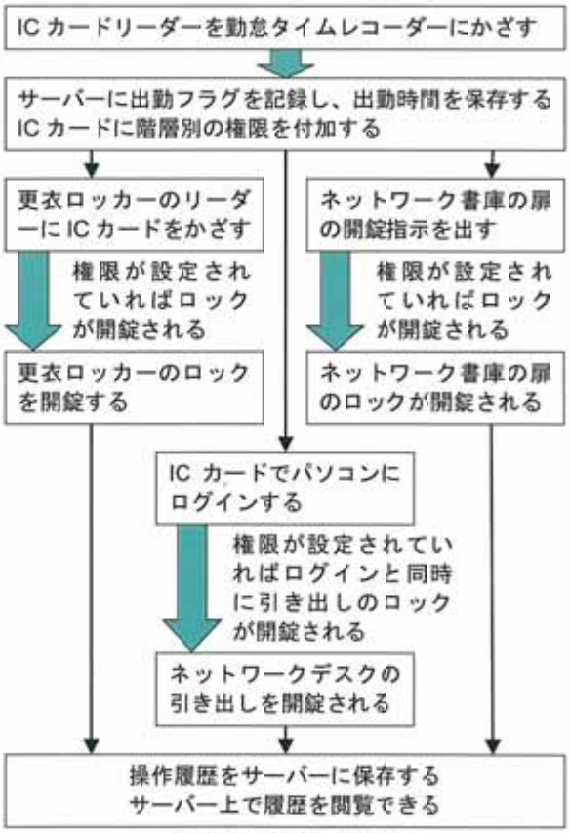


図 30 システム運用

3.3.2 ログインシステム及びサーバ管理システム

ログインシステム及びサーバ管理システムは AdminModule により制御される。図 31 にその構成を示す。

管理アプリケーションは、セキュリティシステムの設定を画面上で行うことができるツールである。管理アプリケーションでは、ドメインユーザ・グループに対して、サーバ上のファイル・ディレクトリ、セキュリティハードウェアへのアクセス権を付与したり、アクセスを監視するための監査の設定を行う。また、セキュリティシステムの運用ログの管理、監査の設定により取得した監査ログの管理、ドメインユーザのカード ID 管理を行う。

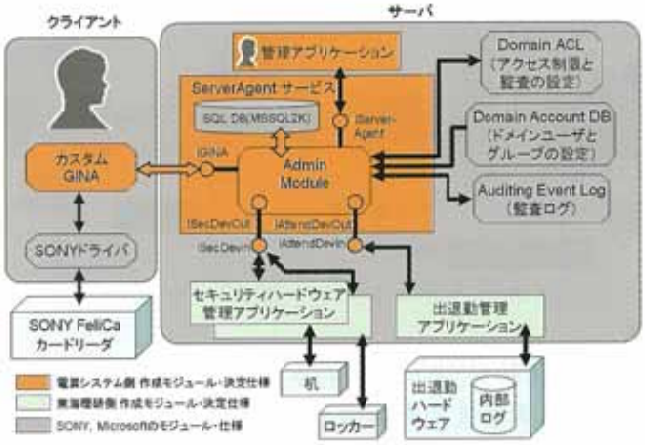


図 31 ログインシステム及びサーバ管理システム

3.3.3 ネットワークデスク

このシステムは、個人のデスクの引出を非接触 IC カード等の本人照合装置を使用し、引出を電磁錠で施解錠を行うことで、引き出しに保管する書類等を本人又は管理者以外取り出せないように管理し、利用履歴はネットワークを経由してサーバに保存することで使用者の特定を行うことができる。鍵のかけ忘れ、鍵の保管義務による過失等の事故を未然に防ぎ、重要な情報を保護する。

システム構成は 2 タイプである。システム 1 は、パソコンに非接触 IC カードリーダーを接続し、パソコンのログインと同時又は、任意にアプリケーションを起動させてデスクの電磁錠の施解錠を行う。カードをカードリーダーから外したり、パソコンのログインを停止及び電源断を行うとデスクの電磁錠が施錠さる。システム 2 は、非接触 IC カードリーダーをデスクに設置し、カードを提示により電磁錠の施解錠を行う。システム 1 、システム 2 共にサーバ管理が可能で、使用者権限の設定、履歴の収集可能である。又システム 2 に関してはスタンドアロンでの運用も可能である。

このシステムの特徴を以下に述べる。

1) 非接触 IC カードリーダーは USB を利用してパソコンに接続し、カードの ID 情報をサーバに照合することで、ID を一元管理できる。又引出施解錠、ログイン履歴を保存することができる。

2) 非接触 IC カードをリーダーから外すと自動的に引き出しが施錠され、パソコンがログオフされる。万一引き出しが開いていた場合は、警報を出す。

3) ID 情報、使用履歴はサーバで管理し、ID 情報の変更及び履歴の閲覧が簡便に行える。

4) 停電等の非常時は非常解除キーを使用し引出しを解錠可能である。ただし、電源供給されていない状態で非常解除キーを使用した場合、履歴は残らない。電源供給されている場合は、「こじ開け」として履歴が残る。

システム 1 の構成と運用を図 32 に示す。

1．IC カードが提示されたらサーバに問い合わせる。
（権限が無い場合はエラーを返す）
2．権限が設定されていれば解除許可を電磁錠制御機に送る。

3．電磁錠制御機は解除許可されたデスクの電磁錠を解錠する。

システム２の構成と運用を図 33 に示す。

1．IC カードが提示されたら電磁錠制御機に問い合わせる。
（設定されていない場合はブザー等のエラーを返す）

2．権限が設定されていれば解除許可されたデスクの電磁錠を解錠する。

3．履歴情報を LAN 経由でサーバーに送る。

スタンドアローンでの運用が可能である。

図 32 ネットワークデスクシステム 1

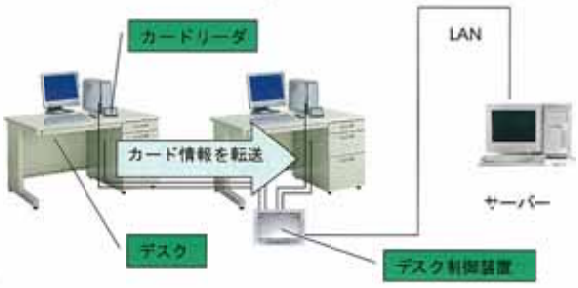


図 33 ネットワークデスクシステム 2

3.3.4 ネットワーク書庫

このシステムは、書庫に非接触 IC カード等の本人照合装置を使用し、引き出し、扉を電磁錠で施解錠を行うことで、書庫に保管する書類等を取り出し権限を付加された IC カードの提示時以外は取り出せないように管理し、利用履歴をネットワークを経由してサーバに保存することで使用者の特定を行うことができる。書類等の重量物の不正取り出しを防ぎ重要な情報を保護する。ネットワーク書庫の構成図を図 34 に、その外観を図 35 に示す。ネットワーク書庫に非接触 IC カードを提示すると、ID 情報がサーバに登録される取り出し権限が付加されているか識別し、権限が特定できれば書庫の電磁ロックを外す。

システム構成は 2 タイプである。システム 1 は、書庫に装備されたコントロールパネルから書庫の施解錠を行い、コントロールパネルに履歴を保存すると同時にサーバに履歴情報を送る。システム 2 は、パソコンから解除指示を発信すると、サーバの権限情報に基づき書庫の施解錠が可能である。システム 1 、システム 2 共にサーバ管理が可能で、使用者権限の設定、履歴の収集可能である。又システム 1 に関してはスタンドアロンでの運用も可能である。

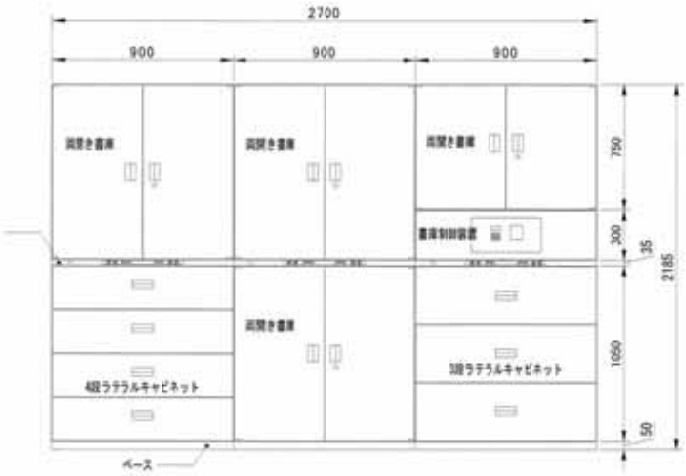


図 34 ネットワーク書庫構成図

図 35 ネットワーク書庫外観

このシステムの特徴を以下に述べる。

1) 制御ユニット 1 台で、RS-485 を使用し書庫 16 セットまで接続可能。
2) 書庫は引き出し式、扉式、引き違い戸式の組み合わせが可能。
3) 制御ユニットにメモリーを搭載し、スタンドアロンで動作可能。また、管理パソコンから ID 情報をアップロード、履歴をダウンロードできる。
4) 停電等の非常時は非常解除キーを使用し引出しを解錠可能。電源供給されていない状態で

非常解除キーを使用した場合、履歴は残らない。電源供給されている場合は、「こじ開け」として履歴が残る。

5)　こじ開け発生時警報ブザーを鳴らす。

6)　閉め忘れブザーを搭載し、設定時間以上開かれた場合ブザーを鳴らす。

システム１の構成と運用を図 36 に示す。

１．IC カードが提示されたらサーバに問い合わせる。
（権限が無い場合はエラーを返す）

２．権限が設定されていれば解除許可をコントロールパネルに送る。

３．コントロールパネルは解除許可された書庫の電磁錠を解錠する。

４．コントロールパネルを使用するとサーバーを接続することなくスタンドアローンでの運用が可能である。

システム２の構成と運用を図 37 に示す。

１．クライアントパソコンから書庫解除の要求が LAN を経由してサーバーに入ると権限を確認し許可する。

２．権限が設定されていれば解除指示を書庫制御装置に送り書庫の電磁錠を解錠する。

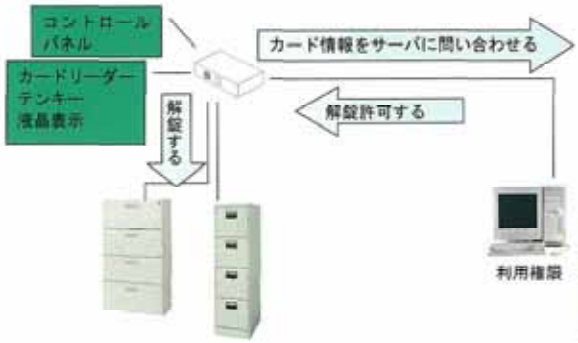


図 36 ネットワーク書庫システム１

図 37 ネットワーク書庫システム２

3.4 小括

グループ階層ネットワークを使用した本人照合機能の研究に当たり、IC カードを媒体として本人照合を行うシステムの研究を行った。グループ階層化は、横割に部門、縦割に役職をマトリックス状に構成することで、細かな権限設定を行うことが出来る。権限設定を行うことで、勤怠、入退室等の人の管理、サーバ等の電子媒体の情報管理、保管庫等の財産及び物の管理をトータル的にセキュリティをかけることが可能なシステムを構築した。

IC カードでの本人照合の場合、暗証番号を利用したとしてもなりすましが可能である。なりすまし防止の為に、顔又は、指紋等個人の特徴を照合する手法が必要である。顔照合技術は現在研究中で、個人特定までは行えないが、顔を顔として認識する技術レベルは向上してきた。しかし現段階では市場に対応できるレベルまで上がっていないため今回の研究は IC カードを媒体とした。

フェーズ III

今後の取り組み

これまでの研究において、顔認識を応用したシステムの構築を行った。現在のところ顔照合は、設置環境により認識精度が左右されている。個人によっても差が発生するため、今後照合精度を向上させる上で、顔データの更新のタイミング、しきい値の決定、動作環境の決定等未確定要素が多々あるので、引き続き研究を行う。

動線検知に関しては、環境により精度が左右される。カメラアングル、被写体の大きさにより左右されるため、調整が困難な状況である。今後、動きだけでなく、静止画上の認識もマッチングさせ２重のチェックを行う事とカメラアングルによっての人物認識の確実性の研究を行う。今後上記した条件、特に外光の影響に左右されないシステムの開発を目指し研究を進める。

ネットワークシステムとしては、今後サーバー管理システムとネットワークスタンドアローンシステムの2タイプの展開を想定している。サーバー管理システムは、ネットワーク上に接続される各機器から直接ICカードのID情報をデータベースにアクセスし権限を取得する。権限はデータベースで付加され、ID情報と履歴をサーバで管理する。ネットワークスタンドアローンシステムは、ネットワーク上に接続される各機器がスタンドアローン（各機器に単独で制御するCPUを搭載）で動作し、各ネットワーク機器間をサーバ経由若しくは、機器間で直接操作権限を設定する。このようなネットワーク上に接続される機器の構成に影響されることなく、フレキシブルなシステムの構築を目指す。

さらにフェーズIIIでは、写真判別機能付きICカード対応顔認証システムの開発に取り組む。これは赤外光の照度差から図38のような顔の表面方向を得ることで、写真と人物を判別する機能を実現し、高精度なセキュリティシステムの開発を目指している。

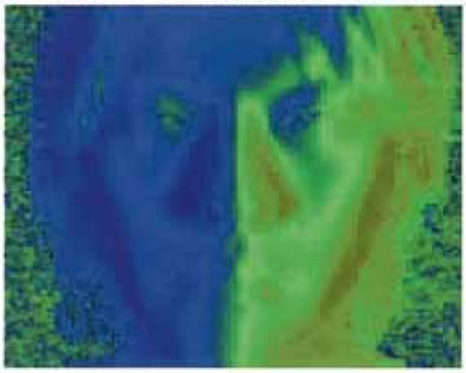


図38 近赤外光照度差ステレオによる顔の表面方向画像