解説

認証技術の現在と未来

坂野　鋭 sakano@rd.nttdata.co.jp，中村逸一 naka@rd.nttdata.co.jp

（株）NTT データ技術開発本部マルチメディア技術センタ

「認証する」とはどういうことか

ここ数年，なんだか耳慣れない「認証」という言葉を耳にすることが多くなった．どうも電子商取引とかいった文脈で用いられることが多いようであるが，その正確な意味はどのように考えればいいのであろうか？

よくある手法で恐縮だが，国語辞典を引いてみると「認証：一定の行為または文書が正当な手続き・方式でなされたことを公の機関が証明すること．（以下略）」とあり，認証の例として，天皇による批准された条約の認証，公証人による会社定款の認証といった行為が挙げられる．なんだか電子商取引とかいった手軽な話ではない様子である．

では，我々が問題にしたい「認証」とはいったい何だろう？　電子商取引に関する海外の文献を調べると現在，この世界で使われている「認証」という言葉は“Person authentication”という言葉が対応しているらしい．これならば「本人であることを確認すること」であり，そんなに重い意味ではなく，電子商取引などの話題にさして違和感はない．本稿では，この「本人であることを確認すること」の意味での「認証」を実現したり保証したりする技術について概論的に解説する．まず，本章では認証することの意味を再確認し，次章以降はこの認証を自動化する技術について解説する．まず，ネットワーク社会，電子社会で考えられる犯罪のパターンとそこで用いられる認証技術を，次に物理的な世界での認証を自動化するバイオメトリクスに関する技術を，さらにバイオメトリクスのうち，なぜか本誌の特集[1]で扱われなかった顔画像の認識技術について解説することにする．

さて，我々は通常「認証」という行為をどのように行っているであろうか？　日常生活ではたとえば現在対面して，あるいは電話で話している相手を確認するためには相手の顔，声，しぐさなどの特徴を用い，無意識に認証行為を行っていると考えられる．一方で，意識的な本人の確認が必要になるシチュエーションは主に公共機関や金融機関のように，サービスそのものが不特定多数の人物に対して行われ，かつサービスを受ける個人が特定されなくてはならない場合である．つまり，知らない特定個人との取引，サービスなどが存在する場合とまとめることができるであろう．このときにはどのような認証手段が用いられているであろうか？　たとえば，銀行で預金をおろすときは預金通帳と印鑑が認証に用いられている．また，市役所などの窓口では主として印鑑が認証に用いられている．これらは，印鑑，通帳などの所有物を持っている人を本人と認めるという方法である．これに対して，ATMなどではキャッシュカードと暗証番号が用いられ，一般的なコンピュータシステムへのログインのためにはパスワードの入力を要求される．これらは，何らかの知識を持っている人物を本人だと確認する方法である．一部のテレフォンバンキングでは申請者の住所，氏名，電話番号，家族構成，家族の誕生日などの情報を本人確認のために用いているが，これも知識を用いた認証と位置づけることができるだろう．

しかしながらこれらの認証方式には，いくつもの問題点があり，事実いろいろな局面で問題を引き起こしている．たとえば，市役所の窓口で住民票を不正請求する犯罪は年間で数百件発生しているし，最近では不正取得した住民票を用いた運転免許証の不正請求事件にまで発展している[2]．

こうした犯罪はいかにして引き起こされているだろうか？　比較的数多く見られるケースは単純に電話帳などで被害者の住所を調べたうえで市販の印鑑を購入し，素知らぬふりをして住民票を請求すればOKである．つまり，技術的にはまったく無防備に近いといってよい．

一方で，キャッシュカードも決して安全とはいえない．キャッシュカードは一応暗証番号で守られているが，実は，かなりの人々が暗証番号として誕生日や電話番号などの覚えやすい番号を用いている．このため同時に盗まれた保険証などから容易に暗証番号を見破られてしまうのである☆1．

☆1　一般に盗まれたキャッシュカードの暗証番号のおよそ2割が解読されてしまうと考えられているが，2割で済んでいるあたりが日本の治安のよさを表しているのかもしれない．

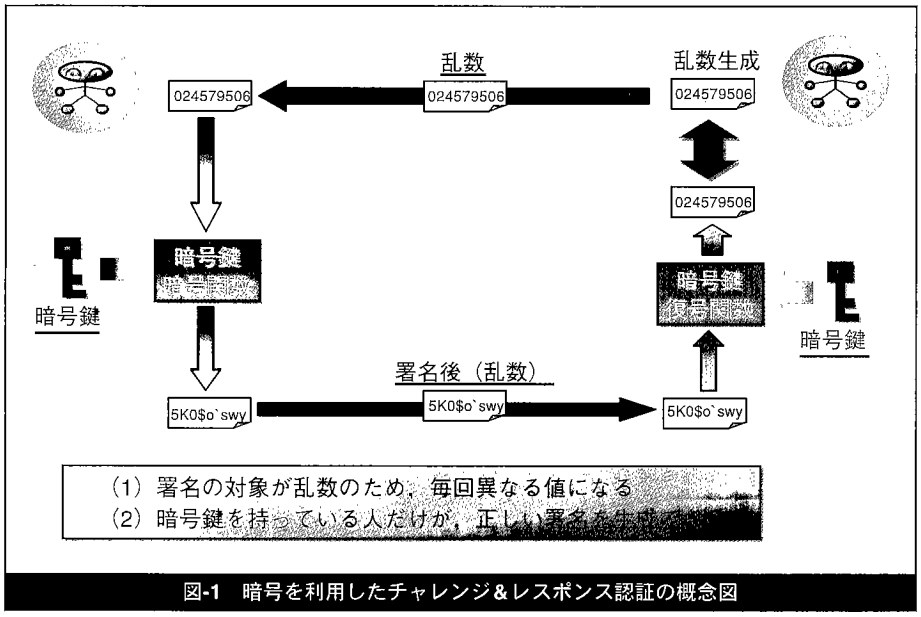

図-1　暗号を利用したチャレンジ&レスポンス認証の概念図

日常生活で使われる認証方式である所有物による認証，知識による認証は共に，相手しか持っていないものを確認することが前提となっている．インターネットで印鑑などを送ることはできないので，知識による認証が唯一の手段となる．通常，本人しか持たない知識として用いられるのはパスワードだが，数文字のパスワードがきわめて脆弱であることはよく知られている．また，盗聴による漏洩の危険も存在する．

そこで用いられるのが暗号である．単純にいえば，通信の際に，双方が鍵と呼ばれる暗号コードを持つことで，当事者以外には平文に戻すこと（この操作を復号という）ができない暗号文を交換することで当事者であることを確認できるわけである．

これまでの例で実世界のサービスでさえ，本人認証が必ずしも簡単なことではなく，現状の認証方式が著しく不完全であることが理解していただけたことと思う．しかも，市役所，銀行の双方の例は電子申請，インターネットバンキングの形でインターネット上に実現しようとしている．そこではどのような認証手段が必要とされているのだろうか？　次章では，インターネット上での犯罪の可能性とその対策としての電子認証方式について解説する．

電子認証方式[3)]

➡インターネットにおける偽装と暗号

インターネットに限らず，電子情報を用いた伝達には1つの共通の課題がある．すなわち，電子情報はきわめて簡単にコピーすることができ，しかもコピーとオリジナルを区別することが不可能，というより区別することに意味がないということである．また，改竄された情報についても改竄されたという事実自体を検出することがきわめて困難，もしくは不可能である．

つまり，電子商取引，電子申請においては，現在起こっているタイプの，本人に成りすますことで，あるいは偽造を行うことで成立する犯罪がきわめて容易になってしまうということである．また，たとえば，現実世界に店舗を開くことはそれなりにお金も時間もかかるが，インターネット上に店舗を出すのは極端にいえばHTMLを数行書くだけの手間でよく，はるかに簡単である．したがって，インターネット上ではコストの観点から従来は考えられなかったタイプの新しい犯罪さえもが成立し得るということである．

それでは，認証つまり，相手が本物であることを証明するためにどのような方法が考えられるであろうか？

簡単な例として携帯電話の認証などで使われるチャレンジ&レスポンス方式による認証を説明しよう．**図-1**に示すように，端末からネットワークに対して認証請求が行われると，ネットワークは乱数を発効する．端末側では，その乱数に対して暗号化を施し，暗号をネットワークに送る．ネットワーク側では端末から送られた暗号を解読し，送った乱数と一致しているかを確認し，一致すれば正当なユーザであると認める．つまり，正当な暗号化鍵を持たないユーザは，与えられた乱数に対し，正当な暗号化を行うことが不可能であるため，システムの不正使用は不可能になる．また，用いられるチャレンジは毎回異なる乱数であるため，盗聴などの方法で成りすますことも困難である．

これで，十分な認証手段が確保されたかに見える．しかし，問題はそう簡単ではない．すぐに思いつくのは，正当なユーザに暗号鍵をどのようにして渡すかである．携帯電話の場合には出荷時に暗号鍵を入力しておけばよいが，インターネット上の電子商取引などでは不特定多数のユーザに個別の暗号鍵を配布する必要が出てくる．無論，インターネットで暗号鍵を配布するわけにはいかない．また，1対1の通信では問題にならないが，ユーザが増加した場合，対応する鍵をどのように管理するかも大きな問題になってくる．これらの問題を解決するのが公開鍵暗号方式である．

➡公開鍵暗号

暗号は大きく共通鍵暗号と公開鍵暗号の2種類に分類することができる．共通鍵暗号は暗号化と復号の2つの操作を1つの鍵で行う方式で，DES，FEALなどがこれにあたる．このような，暗号化と復号を1つの鍵で行う方式を「共通鍵方式」と呼ぶ．これに対して，**図-2**に示すように，RSAなどの公開鍵暗号方式

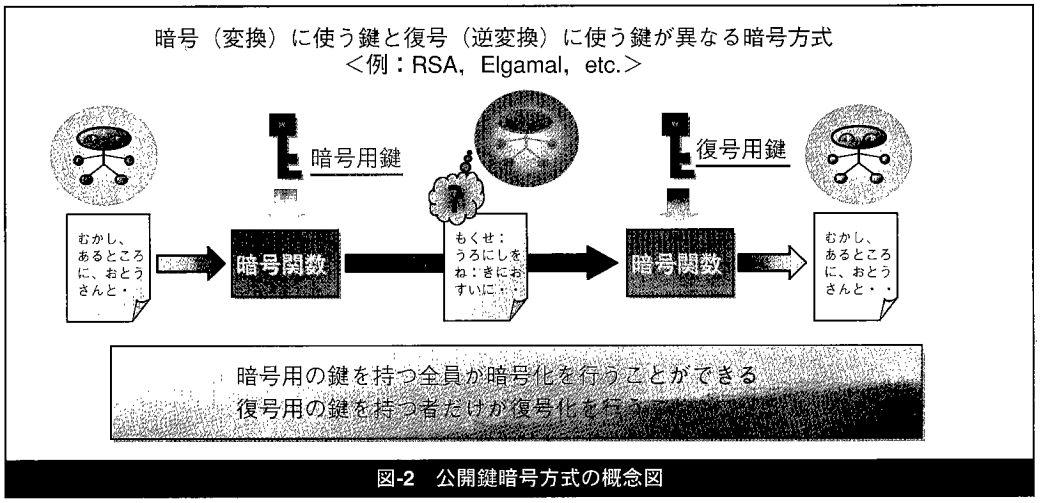

図-2　公開鍵暗号方式の概念図

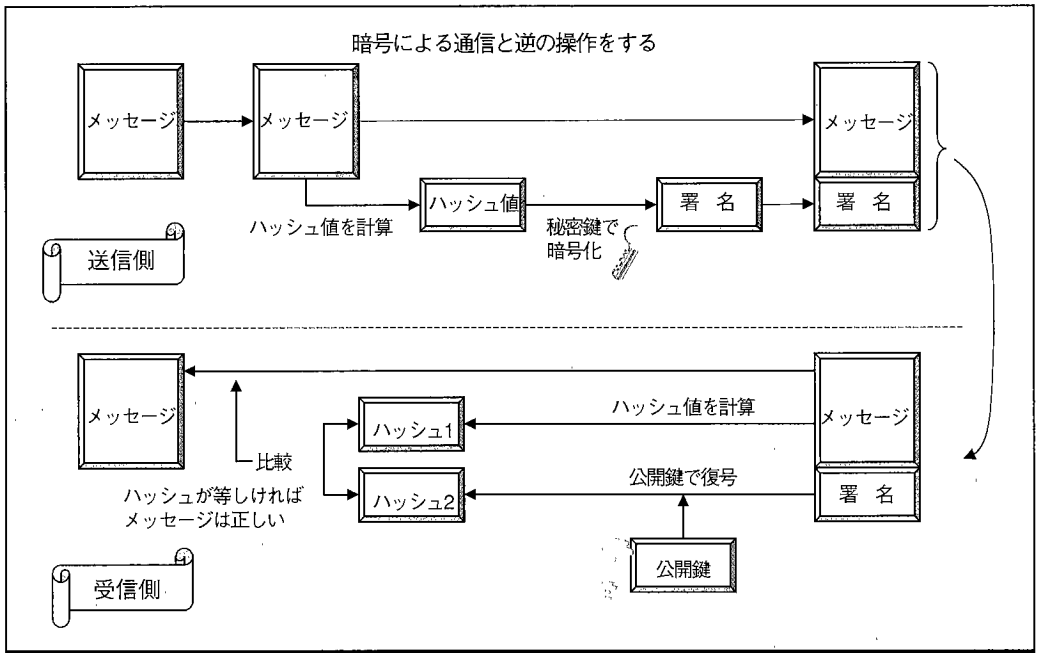

図-3　電子署名のしくみ

では，暗号化する鍵と復号する鍵の2種類の鍵を用いる．この方式を用いると，たとえば暗号通信を行う場合には，暗号化鍵を公開とし（このため公開鍵暗号方式と呼ばれる），復号鍵のみを自身が秘密に管理することにより，事前の鍵交換を必要とせずに暗号通信を行うことが可能になる☆2．この性質を利用すると，インターネット上でさまざまな認証方式が可能になる．

➡電子署名

最も基礎的な電子認証技術が電子署名である．署名（サイン）は特に欧米では本人しか作ることができない文字列として認証に用いられているわけだが，電子署名は，これをディジタル情報として実現する．基本原理はごく簡単で，暗号通信の場合とは逆に暗号鍵と復号鍵のうち，復号鍵のみを公開とする．こうすると，暗号化操作を行うことができるのが本人のみとなるため第3者による偽造のみならず，受信者による改竄も不可能となる．電子署名による認証の流れを**図-3**に示す．

しかし，これでもまだ安心とはいえない．というのは，暗号鍵自身が果たして正当な相手から配布されたものなのかを保証されていないからである．このことが保証されないと，公開されている暗号鍵の生成法を用いて，初めての相手に対して，あたかも電子署名を用いたかのような偽造を行うことが可能になってしまう．この問題を回避するためには，発効されている暗号鍵が正当なものであることを保証する必要が出てくる．そこで，用いられるのがCA－Certification Authority－第3者認証局の仕組みである．

➡CA

用いられている暗号鍵の正当性を保証するためには，何を保証すればよいであろうか？

この疑問の回答は実世界にある．たとえば，日常

☆2　よく，公開鍵暗号の方が共通鍵暗号より機密性が高いという誤解を目にするが，公開鍵暗号方式では，原理的には，公開鍵を解析することにより，秘密鍵を割り出すことができる．これに対して共通鍵方式では暗号化された文書の統計情報を用いた解析しか行えないため，攻撃は公開鍵に対するより困難である．

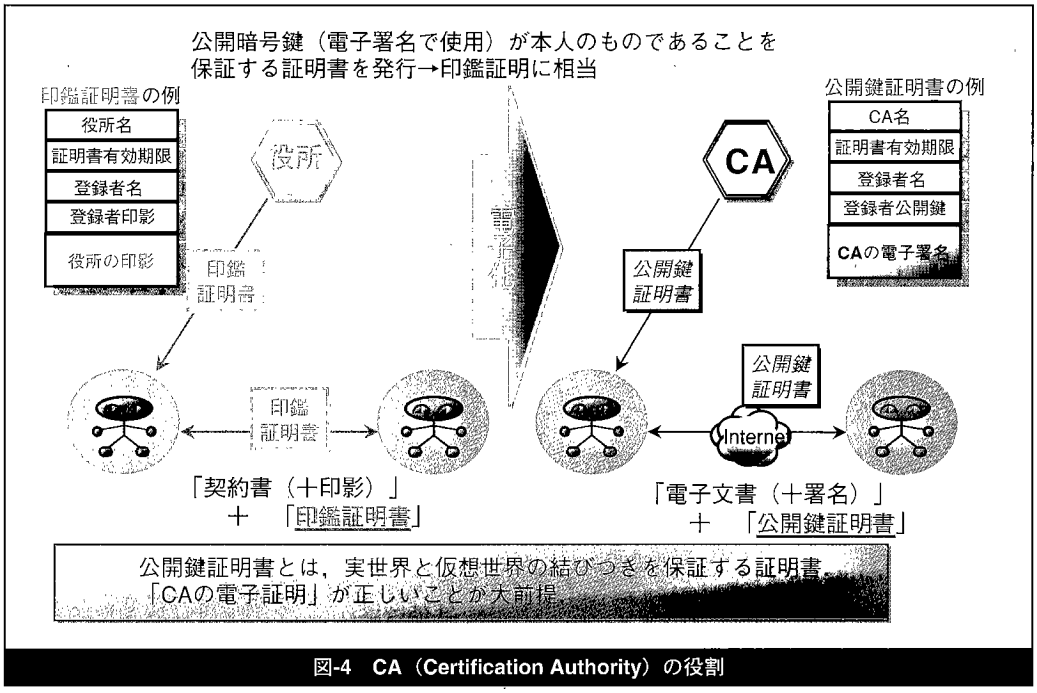

図-4　CA（Certification Authority）の役割

用いている印鑑の正当性，つまり，確実にこれが本人を示すもので同名の印鑑を入手したものではないことを示すには，市役所で「印鑑登録」するという方法が用いられている．つまり，公的な機関に印鑑の正当性を保証してもらうことである．

電子社会，インターネット社会でいわば市役所の役割をするのがCA－「Certification Authority」である．CAは公開鍵証明書の発行・管理機能を有し，公開鍵の正当性を保証する．**図-4**に市役所とCAを対比して流れを示してみた．

なお，ここで用いられる公開鍵証明書とは，公開鍵暗号方式における公開鍵に対してその所持者情報や有効期限などの利用時に必要な情報を付加した電子データであり，その完全性はCAの電子署名により保証される．証明書の内容に関しては，現在ITU-T勧告X.509に準拠したものが一般に使われており，異なるシステム間の相互利用性の実現には，事実上X.509準拠が必須となっている．

公開鍵の配布では，対となる秘密鍵の所持者の特定性の確保が必要となるが，証明書を用いることにより，CAを信用しさえすればオープンな通信路上でも配布が行えることになる．つまり，CAが秘密鍵所有者の物理的な存在を保証するわけである．

しかし，証明書を発行する機関であるCAはシステム全体の信用を保証するきわめて重要なインフラとなるため，ここが誤りを犯すとCAを信用して構築，運用が行われているシステム全体の安全性が揺らぐことになる．

したがって，CAには厳密な運用とセキュリティ確保が要求される．まず，当然のことながらCAの秘密鍵の漏洩は発行した全証明書の信用の低下につながるため，厳重に守られる必要がある．次に，証明書の発行に際しては，成りすまし防止のために申請者の本人確認が必要となる．また，その証明書自体が何らかの許認可を意味する場合には，その資格審査も必要となる．

また，通常，証明書はCAの設定した有効期限まで利用可能だが，何らかの理由で証明書を失効する際には，その証明書の利用者全員にその事実を通知する必要がある．このためよく用いられるのはCRL－Certificate Revocation Listと呼ばれる失効リストを公開する方法である．

また，CA自体の信用性を誰が保証するかという問題に関しては，CAの信頼性を保証する上位のCAを用いる方法が検討されている，無論，その上位のCAの信頼性を誰が保証するかという無限階層が存在するわけだが，その最終的な階層は恐らく，国家，政府のレベルでのCAで保証されることになる．このような階層構造の最上位のCAをルートCAと呼ぶ．このような仕組みの整備によって，国家の信頼性に基づく，安全なネットワーク取引，申請などを実現するための技術が整備されている．

物理世界との接点－バイオメトリクス

これまで電子的に認証を可能にする仕組みについて概説してきた．しかしながら，よく考えて欲しいのは，たとえば最初の携帯電話の例でいえば，チャレンジ＆レスポンス方式の認証により携帯電話が正当であることは認証されているが，その携帯電話を使っている人が，正当な利用者かそれを拾った，あるいは盗んだ人物かは認証されていないということである．

つまり，電子的な世界へのアクセスの入り口はやはり物理的なものであり，物理的な認証方法を考慮しなくては，電子的な世界の認証も成立しないということである．現在，実世界の認証方式として用いられているのは，先にも挙げた

生体特徴	特　色	適用例
指　紋	高精度．最も歴史がある	犯罪捜査，国家ID システム，福祉など
虹　彩	高精度．急速な拡大	ATM
網　膜	高精度	刑務所，福祉など
掌　形	ユーザ受容性高い	入出国管理，医療など
顔	最も自然．精度は低い	入出国管理，福祉など
音　声	自然．電話で使用可能	テレフォンバンキング，RAS 認証
筆　跡	欧米では自然． 急速な低価格化	失業保険認証
耳形状	意外と高精度	研究中
歩き方	低精度	研究中
血管分布	高精度	製品が発表された
DNA	血縁の特定が可能	研究中

表-1　いろいろなバイオメトリクス

- 所有物による認証
- 知識による認証

の2つの方法であるが，双方ともインターネットの世界で確実な認証を行うためには少々問題がある．たとえば，ICカードのような解読の困難な媒体に暗号鍵を保存することにより，認証を行う仕組みは有効そうに見えるし，事実ある程度有効ではあるのだが，携帯電話の例と同様，ICカードを持った人物が正当なユーザであるかどうか確認したことにはなっていない．

そこで，次のレベルで用いられるのが，パスワードや暗証番号に代表される秘密の知識を用いた認証である．しかしながら，こうした知識による認証方式はさまざまな方法で簡単にその秘密を突き止められてしまう．たとえば，最も単純な方法は肩越しにパスワードを打っているところを盗み見る方法である．少々高級な方法とはいっても，本人，家族の氏名，誕生日，単語辞書などから類推する方法であり，決して誰にも真似のできない方法ではない．

また，秘密情報を用いた方法は必ずしもユーザにとって利便性の高い方法とは言い難いらしく，たとえば，携帯電話には暗証番号で機能をロックする機能がついているが使っている人はあまり見たことがない．

そこで，現在，急速に注目を集めているのが，人間の生体的な特徴から機械が人物を自動的に認識する技術－バイオメトリクスもしくはバイオメトリック個人認証技術と呼ばれる技術である☆3．

バイオメトリクスに関する個別の議論，標準化の動向などについては本誌1999年11月号の特集「ここまできたバイオメトリクスによる本人認証システム」や他の一般的な解説[1),4)]に譲るとして，ここでは，概論的な意味でバイオメトリクスがどのように役に立つかを解説することにしよう．

☆3　英語ではBiometricsもしくはBiometric Person Authenticationであるが，現時点（2000年4月）では確定した訳語は存在しない．本稿では「バイオメトリクス」という言葉を用いることにする．
☆4　もっとも，指紋，顔，音声，筆跡などのバイオメトリクスがきわめて低価格化している昨今，こうした問題は単に好みの問題になってしまうかもしれない．

➡バイオメトリクスのいろいろ－何がどこで役に立つのか

現在利用可能もしくは研究中のバイオメトリクスは，**表-1**のようにまとめることができる．

どの技術においても，カメラ，スキャナ，マイクロフォンなどの入力装置から入力した指紋，顔などの生体特徴と，事前に登録されたテンプレートと呼ばれるデータとを比較し，十分に類似していれば本人と認めるという意味では同一である．これらの生体特徴を自動認識することにより，本人認証する技術は，

(1) 生体特徴なので基本的に盗むことができない
(2) ユーザはパスワードなどを記憶する煩わしさから開放される

という，2つの顕著な特徴を持つ．

恐らくこうした表を初めて見る人の最も単刀直入な疑問は，「結局どれが一番いいのか？」と「なぜここまで多様な技術があるか？」ということであろう．これらの疑問に答えるには，バイオメトリクスが共通に持つ課題を挙げる必要がある．

バイオメトリクスは生体特徴を用いた認証方式であるから，人間の状態，センサに対する雑音のため，いつも同じ信号が入力されるとは限らない，このため，認証精度は必ずしも100％となることが保証されない．また，損傷などの理由で特定個人の生体特徴が失われ，使えないユーザが存在する場合も考えられる．つまり，バイオメトリクスの課題は

- 認証精度は絶対に100％にならない
- すべての人が使える生体特徴は存在しない

の2点に集約される．

特に，後者の課題は，使用する環境条件に大きく依存する．たとえば，手袋をつけることが不可欠な職場では，指紋認識技術は必ずしも使いやすい技術にはならないし，騒音の激しい環境では声紋技術を使うことは現実的ではない．このように，どのバイオメトリクスが最適かは，状況によってかなり左右される．このほか，認証装置のコストとセキュリティレベルのトレードオフを考えることは常に重要である☆4．

これらのことをまとめると

- あらゆる状況に最適なバイオメトリクスは存在しない

ということになる．無論，システムのセキュリティレベルによっては，単一のバイオメトリクスだけでは要求精度を達成できず，複数のバイオメトリクスを用いる場合も考えられるし，そうした検討も行われている[5)]．

また，少々逆行するように感じられるが，ICカードなどの所有物との組合せは現実的な解である[6)]．所有物との組合せでは，本人排除率を下げることはできないが，他人受入率は，大幅に低下する．このような場合には，たとえば他人受入率が10％だったとしても，従来のシステムと比較して確実にセキュリティレベルが上がる．バイオメトリクスにおいて

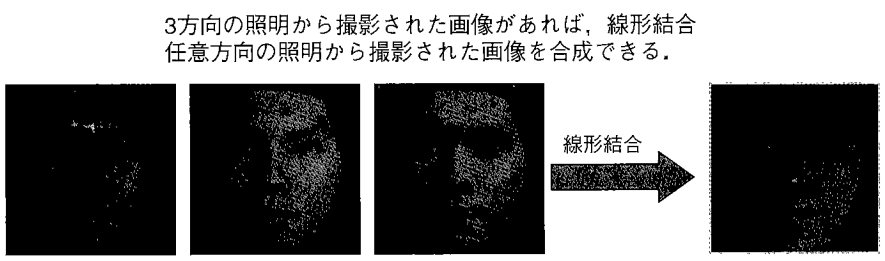

図-5　Illumination Cone法の原理

現状最も問題なのは，「どういう使い方をするか？」ということなのである．つまり，使い方を間違えなければ，バイオメトリクスはあらゆる情報システムをセキュリティレベル，ユーザビリティの双方の観点から改良する技術なのである．

顔画像の認識技術

顔画像の認識技術を応用した認証技術は，

(1) 被認証者にまったくもしくはほとんど意識させずに認証動作が可能である
(2) 光学系の増設により，相当遠距離からでも個人の同定が可能である

という観点で，さまざまなバイオメトリクスの中でも，顕著な特徴を持っている．また，社会的にも，「顔が一致すれば本人と認める」ことはほぼ一致した認証手段といっていいことからユーザ受容性の高い手法と考えられる．

こうした観点で，顔の自動認識技術は多くの研究者の関心を引いてきた．顔画像の認識技術が活発となったのは1991年にMITのM. Turkらが発表した“Recognition Using Eigenfaces”（固有顔による認識）というちょっと風変わりなタイトルの論文がきっかけであった[7]．

この論文は統計的パターン認識の古典的な手法である，部分空間法[8]を顔の認識に適用しただけのものであったが，その影響は大きかった．この論文の大きな意義は，照明，姿勢などの条件を固定すれば顔の認識はあまり大きな技術的工夫を必要とせずに，実現できることを示した点にある．実際，制限された条件の下では，単純に画像を重ね合わせる程度のことでかなりの性能で個人同定が可能であることが実験的に示されてきた．

しかし，研究が進むうちに，顔の姿勢，表情，照明条件などの問題が物体認識のための本質的な問題であることが理解され，近年は，挑戦的な研究課題として多くの研究者を引きつけている．これまでこうした問題を解決するためには多くの手法が提案され，テストされているが，それらの多くについては包括的な解説[9]に譲り，ここでは，筆者流の分類と興味深い研究例を紹介する．

筆者の見解では，顔の認識のために重要な技術は，視覚の計算理論（Computer Vision；以下CV）に基づく方法と，統計的パターン認識に基づく方法の2つである．前者は3次元世界を撮影した際に，画像が生成される状況を順問題として，与えられた2次元画像から3次元世界を再構成することを目標とする理論体系であり，本来3次元物体である顔の認識のためには不可欠である．いま1つの統計的パターン認識の理論は複数のサンプルの統計的な性質から，与えられたデータがどのクラスに属するかを判定するための体系であり，柔軟に変形する顔を認識するための技術として不可欠であると考えられる．

このように双方とも顔の認識に関しては不可欠な理論体系であるにもかかわらず，これらの双方にまたがる研究成果はあまり見られず，多くの研究は顔を剛体と仮定し，厳密にCVの理論を適用する方法と，カメラからの入力画像を単なる信号と捕らえ，統計的パターン認識の理論を適用する方法に2分されている．以下ではこれら2つの方向の研究のうち興味深いものを紹介する．

➡コンピュータビジョンの理論に基づく方法

視覚の計算理論に関しては陰影，テクスチャ（模様），運動などの情報から対象の3次元構造を復元するための各種の方法が提案されている．これらの手法は原理的にはすべて顔の認識のために応用することが可能であり，実際にいくつかの応用例も存在するが，特に興味深いのは，Georghiadesらによる Illumination Coneと呼ばれる光学的な拘束条件を用いた方法である．Shashuaは，単一光源の自由度が3であることに着目し，3枚の照明条件の異なる画像があれば，任意の照明条件の画像を合成できることを示した．Belhumerらは，これによって形成される部分空間をIllumination Coneと名づけた．Georghiadesらは，この部分空間が，物体の照明条件による変化のすべてを包含することに着目し，入力画像とIllumination Coneの類似度を用いて顔を認識する手法を提案し，顔の姿勢を固定し，照明を変化させる実験を通して有効性

を示した（**図-5**）．

この方法は，原理的に照明条件による変動をすべて吸収することができるが，一方で，複数の画像の対応点を厳密に計算する必要があるために顔の姿勢が変動した場合には適用できないという問題があった．この問題に対し，春山らはMakiの提案したGeotensity拘束を用いることにより光源，姿勢変動が存在した場合にもロバストな認識手法を提案している[10]．

上記の手法は，CVの理論の基礎的な側面の検証を行う意味でも意義深いが，一方で，問題を顔の認識に限れば本人の3次元データをレンジファインダなどの装置で採取し，認識時には3次元データから合成された画像と比較する比較的簡便な方法で姿勢，光源の問題に対処する方法も提案されている[11]．

➡統計的パターン認識理論に基づく方法

CVの理論に基づく方法は，多くの場合理論的に美しく，しかも前提条件が満足されている場合には確実に正解を出す意味で優れた手法である．しかしながら，これらの研究では顔が剛体であるという仮定がなされている場合が多く，これは明らかに現実の顔を反映していない．

とはいえ，一方で，個々人の顔がどのように変形するか？　たとえば，どのような表情をし得るか，どのようにひげが生えるか，どのように年をとるかなどをモデル化することは，ほとんど不可能といってもよい（そういう研究も存在しないことはないのだが，うまくいっているようには見えない）．

そこで，用いられるのが，学習データから統計モデルを推定し，未知入力がどの個人かを判定する統計的パターン認識の理論である．統計的パターン認識に基づく顔認識の研究は，多くの場合，登録時に入力された複数の顔画像から，平均，分散，主成分などの統計量を推定し，未知の入力データと統計モデルの類似度を計り，最も類似しているもの，もしくは類似度が事前に定められた閾値を超えているものを本人と認めるという考え方で進められてきた．顔の認識に関する研究ではTurkの論文の影響からか統計モデルとして主成分分析で求められる基底で張られる部分空間を用いたものが多い．

主成分分析を用いることは，与えられた画像群の中から，線形モデルで近似できる不変量を抽出する処理にほかならない．主成分分析を用いた手法の中で筆者らが最も興味深いと考える研究は山口らによって発表された相互部分空間法を用いた顔認識技術である．通常の部分空間法は，登録時に与えられた複数の学習データに対して主成分分析を施すことで不変量となる部分空間を計算し，未知の入力データとの角度，距離などの類似度を計算することで認識処理を実行する．一方で，相互部分空間法では学習データから主成分分析で不変量を計算するところまでは同じであるが，認識時には，複数の顔画像を入力画像とし，これらの入力画像に対して主成分分析を施し，登録された主成分との類似度を計算することで認識処理を実行する．つまり，登録時の画像と認識時の画像双方の不変量を計算することで認識率の向上を図れる優れた手法である[12]．ただし，この方法は，与えられた顔画像の不変量が非線型であった場合には，十分な精度を達成できないという問題を持つ．この問題に対して筆者らは，非線型主成分分析と呼ばれる新しい統計手法を適用するアイデアを発表している[13]．

以上，コンピュータビジョンの理論，統計的パターン認識の理論に基づく興味深い顔画像認識の方法を紹介した．これまで述べたように，コンピュータビジョン寄りの研究では明らかに顔を対象とするには問題のある仮定が用いられ，また，統計的パターン認識寄りの研究では登録時の環境を超えた状況での変化を予測することは困難である．今後，コンピュータビジョンの技術と統計的パターン認識の技術を相補的に用いた技術が顔画像認識を実用レベルに押し上げる力となるというのが筆者の予想である．

認証技術の将来

以上，ネットワーク社会，電子化社会において，申請，商取引などを安全に行うための自動認証技術について概観した．将来はどのような認証技術が現れるか，想像が付かない側面もあるが，いま，この時点では，ネット上の認証は国家CAもしくは省庁を結ぶブリッジCAをルートとした階層CAが用いられ，物理的な世界では複数のバイオメトリクスが適材適所で用いられるようになっていくことはかなり可能性の高い未来に思えてくる．

最後に，本稿の執筆にあたっては本誌のセキュリティに関する連載，特集記事などとの関係を勘案したため，単独では少々バランスの悪い構成になったことをお許しいただきたい．

参考文献

1) 特集「ここまできたバイオメトリクスによる本人認証システム」，情報処理，Vol.40, No.11 (Nov. 1999).
2) 「他人の住民票移して悪用」，AERA, 1998年2月16日号.
3) 今井: 暗号のおはなし，日本規格協会 (1993).
4) 坂野: バイオメトリック個人認証技術の現状と課題，信学技報，PRMU99-29 (1999).
5) 坂野，劉: 多重バイオメトリクスによる個人認証，情処研報，CSEC5-7 (1999).
6) 飯野，岩瀬，坂野，中嶋: 指紋照合機能搭載型ICカードによる本人認証方式，情処研報，CSEC (July 2000).
7) Turk, M. et al.: Recognition Using Eigenfaces, in Proc. Computer Vision and Pattern Recognition, pp.568-591 (1991).
8) 石井，上田，前田，村瀬: よくわかるパターン認識，オーム社 (1998). ＊部分空間法をはじめとするパターン認識については多くの良書があるが，本書は特に優れている．
9) Pentland, A. and Choudbury, T.: Face Recognition for Smart Environments, IEEE Computer, p.50 (Feb. 2000).
10) 春山，坂野，武川: 陰影・幾何拘束を用いた光源・姿勢変動にロバストな顔認識アルゴリズム，信学技報，PRMU98-134 (1998)，およびその中の文献.
11) 石山，坂本，田島: 三次元形状計測装置の開発とそれを利用した物体認識システム，第6回画像センシングシンポジウム予稿集，pp.195-200 (June 2000).
12) 山口，福井，前田: 動画像を用いた顔認識システム，信学技報，PRMU97-50 (1997).
13) 坂野，武川: 核非線型相互部分空間法と顔認識への応用，信学技報，PRMU99-116 (1999).

（平成12年6月5日受付）