平成16年度経済産業省委託事業成果

平成16年度基準認証研究開発委託事業 －2
生体情報による個人識別技術(バイオメトリクス)を
利用した社会基盤構築に関する標準化

（バイオメトリクス個人認証運用における脆弱性への技術的対応）

研究委託先：　京都大学　ＣＯＥ研究員　鷲見和彦

平成17年３月

社団法人日本自動認識システム協会

３．２　バイオメトリクス個人認証運用における脆弱性への技術的対応

３．２．１　背景・目的

バイオメトリクス個人認証は，唯一の物体の保有や，秘密情報の保有などの代わりに本人の生物学的な独自性を用いて本人を認証するものである。バイオメトリクス個人認証は，なりすまし難いという安全性と本人に常に備わっているという利便性が特徴であり，安全な社会の実現には不可欠な認証方法と考えられている。これまでの本人認証手段へのなりすまし・偽造などの詐称事件が増加の一途を辿り、社会的混乱を招く事態となって来ている。究極の本人認証という観点から、今後バイオメトリクス個人認証がさまざまな用途に広がっていくことが予測される。

バイオメトリクス個人認証の普及は、これまで、機密性の要求されるセキュリティルームや秘密の部署などの入退室管理など、小さな単位の個別システムの個人認証という閉じられたシステムへの応用がほとんどであった。しかしこれからは、システムの大規模化・オープン化が進むことが予想されている。パスポートなどの公的個人認証システムが世界的規模で応用されると、バイオメトリクスの登録システムと認証システムが分かれことが予想される。

普及が進むと別の効果として、類似した応用システムが多数存在することが予測される。例えば、ある企業で使われる出入管理用のバイオメトリクス認証システムと同じテンプレート・登録・管理システムをもつ認証システムが、別の集合住宅でも使われるという可能性が出てくる。企業からみると、同じシステムが多数使われることで、問題点の早期の解決などコストダウンと製品の品質の安定化が進むなどの有利点も出てくる。住宅、企業、会員専用の物理セキュリティシステムや、企業の業務系認証システム､電子商取引システム等の情報セキュリティにおいて、この傾向が強まるとものと予測される。

また利便目的のカジュアルな応用が現れてきている。例えば米国のディズニーランドにおいて、シーズンパスの認証に指の長さを利用したシステムがある。入場券・閲覧権・顧客サービスなどのアプリケーションで、トークンを持ち歩かなくてすむといった、ちょっと便利な個人認証にバイオメトリクスが利用されるシステムが増加することが予想されている。

このようなバイオメトリクス個人認証の普及に伴い、システムの大規模化・オープン化が進み、また類似した応用システムが多数存在してくると、バイオメトリクス個人認証用テンプレートの共通化と流通という問題が生じてくる。

テンプレートの共通化・流通の利点としては、以下の点が考えられる。

- 組織間での信用継承が可能となる。パスポートなどで、日本政府の保証を米国政府が利用する、A銀行での保証をＢ銀行でも利用するなどの信用継承である。
- 複数アプリケーションが同じテンプレートを使用することが出来る。そのことによりシステム開発・登録・運用の安定性とコストの低減が図れる。

このような利用動向を背景に、テンプレートの共通化については、国際標準化（ＩＳＯ１９７９４：Interchange format for Biometrics Authentication）が進行中である。しかしテンプレートの共通化・流通においては、以下のような欠点も考えられる。

- 流通段階においてテンプレートの漏洩・悪用の可能性が増大する。
- フォーマットの標準化によりリバースエンジニアリングが容易になる。例えば銀行のシステ

ムを破ろうとしたときに、もっとセキュリティの甘い同一システムを奪い、リバースエンジニアリングにより設計目標や製品仕様を明らかにして、ターゲットの銀行システムを破ることが可能となる。

- 一旦テンプレート情報が漏洩すると多数のシステムを攻撃される可能性が増えるばかりか、もれたバイオメトリクスは回収不能であり、漏れると元には戻せない。
-

さらに、テンプレートの共通化・流通という問題は、個人情報（プライバシー）の保護の問題に関わって来るが、バイオメトリクスデータを保護するための技術的解決策はまだ定着していないと考えられる。

将来、バイオメトリクスの利用技術が普及発展し、便利な社会になる一方で、プライバシーと個人の権利の侵害というあらたな社会問題が発生すると予想される。また、既成社会との矛盾や制約のために問題の解決がより複雑化することもありえる。このような問題を未然に予防するため、法的対応を施して行くことも必要であるが、バイオメトリクス製品側においも設計段階から技術的に対応を施しておくことにより問題発生を未然に防止することも必要と考えられる。

まず、バイオメトリクスシステムに潜む脆弱性の分析により、社会的な問題の発生を予測し、つぎに、バイオメトリクスシステムの社会的安全性を確保するための設計指針と運用指針とを技術的に蓄積して行くことが今後の課題となろう。

また、このようなバイオメトリクスデータ保護の観点から、脅威に対する安全確保のための共通基盤を実現するには，以下の三点が重要である。

- バイオメトリクス特有の脆弱ポイントの明確化
- 脆弱ポイントごとの脅威の評価
- 脆弱性を最小限にする対策の検討

これらの情報を広く共有化することで，安全で信頼性の高いバイオメトリクスシステムの構築が可能になるものと考えられる。しかし一方では，このような情報の共有化により，バイオメトリクスの脆弱性に関する情報が不適切に流通する可能性もある。そのため，脆弱性情報の適切な流通に関する検討も必要となろう。

３．２．２　バイオメトリック認証システムを運用する上での安全性確保の対策技術の検討

現在のバイオメトリック認証システムに対する脅威と脆弱性に関する研究に関して，脅威と脆弱性抽出の考え方，脅威および脆弱性項目，およびリスクを最小化する対策技術について検討する。具体的には，バイオメトリック認証システムモデルに対して，脆弱性項目の指摘，脆弱性の程度と脅威の程度，対策技術と評価検証の必要性などについて検討する。

一般的に，バイオメトリクスでは，顔や手の形状などの外見的な特徴，指紋･掌紋･虹彩･網膜や手静脈などの発生学的にランダムな特徴を持つ身体部位から得られる特徴,あるいは,署名,音声,歩行パターンなどのように安定して現れる行動的特徴などの生体特徴を抽出し，あらかじめ登録された特

徴のデータベース(テンプレートと呼ぶ)との間でパターン間の類似性を評価して，十分類似性が高ければ本人と認証する。これらの生体特徴は，特殊な装置を使わなければ可視化することが難しく，かつ，それを模倣したサンプルの製造や使用が困難であるため，容易に人に教えたり貸し借りができる秘密情報や物証より安全であるとされてきた。

ところが，近年の研究によれば，バイオメトリクス個人認証に対して多くの潜在的危険性が指摘されるようになってきた。

たとえば，本人の協力や不注意により生のバイオメトリクスデータを得ることができれば，ある条件においては簡単にバイオメトリクス認証装置を詐称する人工サンプルを製作できる可能性や，データを詐称される可能性が指摘されている。

また，これまで民間におけるバイオメトリクスの利用は，テンプレートを相互に流通させない小規模の閉じたシステムに限られてきた。しかし、バイオメトリクス個人認証の普及によって，様々な場面でバイオメトリクスが使用されるのに伴い，認証機関自身が不正を働き，テンプレートや個人情報を悪用する可能性をも考慮しなければならない状況が生まれてきた。生のバイオメトリクスサンプルが得られなくても，テンプレートから個人認証を可能にするバイオメトリクスサンプルを復元する可能性も指摘されている。このような危険性に対する対策と共に，バイオメトリクスは一旦第三者に知られてしまった場合に，パスワードと違って新しいものと置き換えられないというバイオメトリクス特有の問題点に対しても対策を考慮する必要がある。バイオメトリクス個人認証においては、バイオメトリクスデータの保護が今後の大きな課題となっている。

ここでは、このような特性をもつバイオメトリクスにおける個人情報の安全性確保について、バイオメトリック認証システムを技術的側面から分析し対策を検討する。

バイオメトリック認証システムモデル図 ３－７ に基づき脅威発生の可能性が想定されるポイントについて、以下のように検討を進める。

バイオメトリック認証システムモデルは、提示された生体情報を取得して電子的なバイオメトリクスデータを出力する入力装置、バイオメトリクスデータの転送、特徴抽出、確認照合、登録の機能および格納されたテンプレート・データベースから構成されるものである。

１．バイオメトリクスデータが漏洩するポイントを特定する

バイオメトリクス認証システムのモデルマップを具体的な以下のようなシステム構成に展開して、バイオメトリクスデータが漏洩する可能性のあるポイントを特定する。

・ローカルシステムの場合
・センターシステムの場合
・クライアントサーバ（センター管理）の場合

２．脅威を分析する

特定されたポイントについて、「登録時の脅威」「定常時の脅威」「運用時の脅威」について検討を加える。

３．対策案と新技術の方向性について検討する

特定されたポイントにおける分析された脅威についての対策案、特にバイオメトリクスに特有の観点からの対策案について今後の技術的方向性を検討する。

バイオメトリクス生データを保存しないで、テンプレートを利用する技術が推奨されているが、同時にテンプレートの保護を可能にする技術が必要とされる。

対策案と新技術の方向性について、次のように検討を進める。

A．既存技術を応用し、すぐに対応可能な対策を検討する

B．既存技術の応用だけでは対策が完璧でない問題点を抽出する

C．新たに考慮すべき新技術の方向性を検討し、今後の進め方を提案する

４．対策の公開

検討された対策案を、国際標準であるＩＳＯ/ＩＥＣ　ＪＴＣ－１　ＳＣ３７　ＷＧ６に対する標準化活動を計って行くための検討を行う。

３．２．３　バイオメトリクス個人認証を運用するシステムとその脅威分析

本節ではバイオメトリクス個人認証を運用するシステムにおける脅威について、図　３－７　バイオメトリック認証システムモデルに基づき、脅威の発生するポイントを抽出するとともに、脅威の内容を明らかにする。

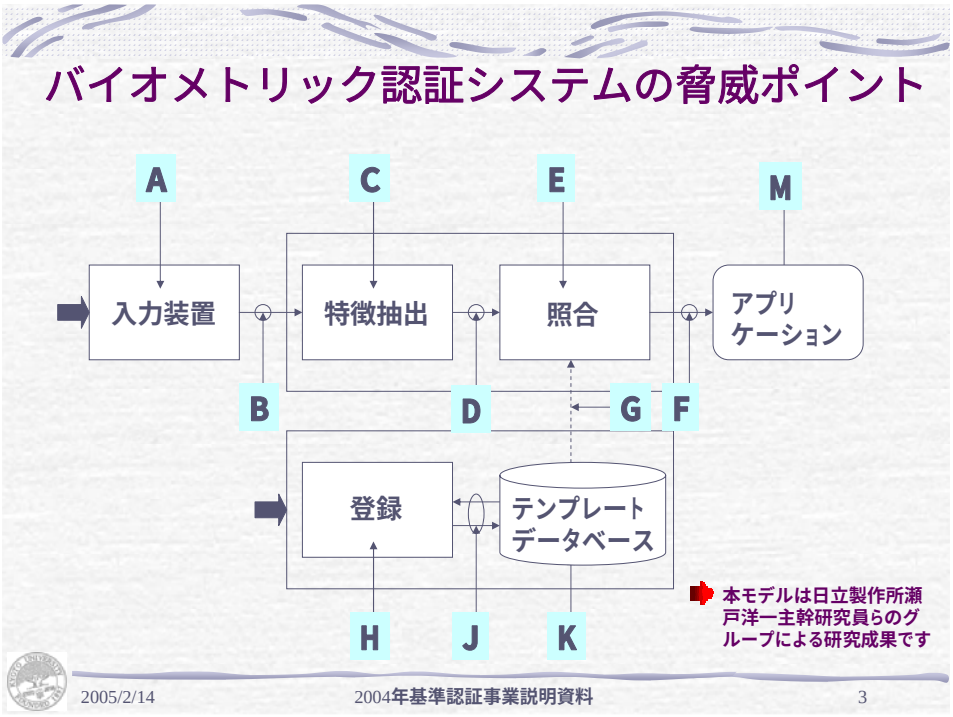


図　３－７　バイオメトリック認証システムモデル

（1）バイオメトリック認証システム登録時の脅威

1）ローカルシステムの場合

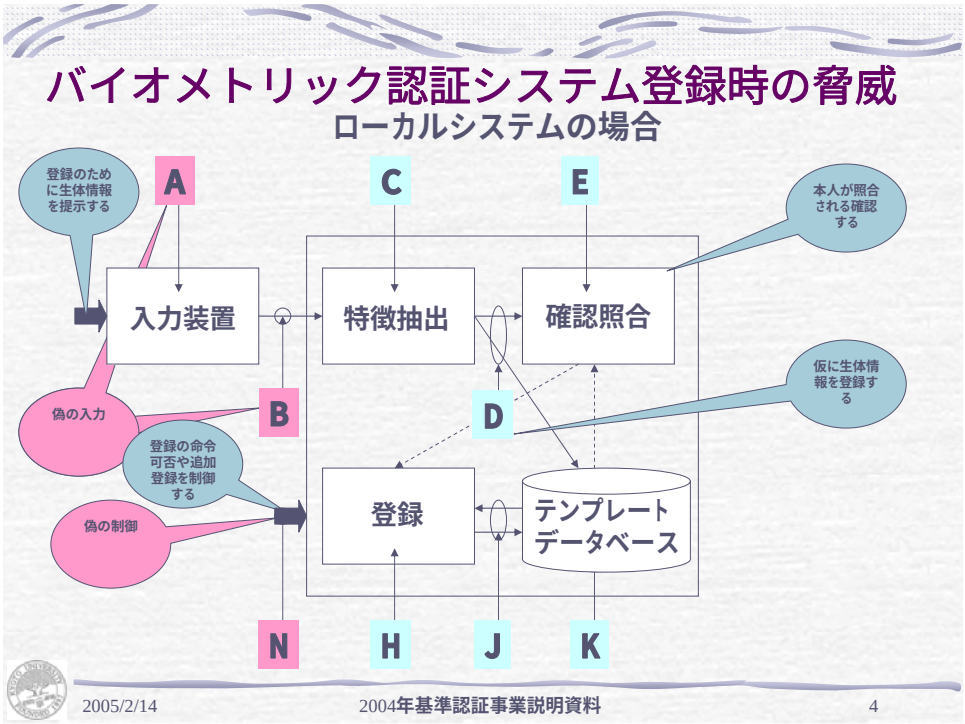


図　3－8　ローカルシステムの登録時脅威

ローカルシステムの場合に、生体情報の「登録」処理において安全性を脅かす脅威の発生するポイントとしては、図 3−8　ローカルシステムの登録時脅威に示されるA、B、Nポイントが想定される。登録時の処理としては、特徴抽出、確認照合、登録があり、データ格納装置としてテンプレート・データベース、およびローカルシステム内の情報通信路がある。

ローカルシステムは一体化された筐体に存在するので、ローカルシステムが物理的にセキュリティの確保がなされていれば、ポイントC、D、E、H、J、Kにおける脆弱性は脅威につながる可能性は低いと想定される。

ローカルシステムにおいては、入力装置における「登録のために生体情報を提示する」Aポイント、入力装置からローカルシステムへの「通信路」Bポイント、および確認された生体情報のテンプレート・データベースへの登録を制御するNポイントが検討するべき脅威発生ポイントと考えられる。

A）　Aポイント：入力装置

登録のために生体情報を提示する入口である。発生する脅威としては、センサへの偽の生体情報の提示がある。人工の生体的特徴によるなりすまし、直前の利用者の残留生体情報によるなりすまし、類似あるいは瓜二つのテンプレートでのなりすま

しなどがある。

B）　Bポイント：情報通信路
登録のために生体情報を転送する部位である。発生する脅威としては、蓄積された生体情報の再入力および入力された生体情報の漏洩がある。

N）　Nポイント：登録処理制御機構
登録の命令可否や追加登録を制御する機構である。発生する脅威としては、装置のモードを不正に変えて、偽の登録を行う登録モードへの不正な移行がある。バイオメトリックスシステムに対する不正な登録によるなりすましの脅威である。

2）センターシステムの場合

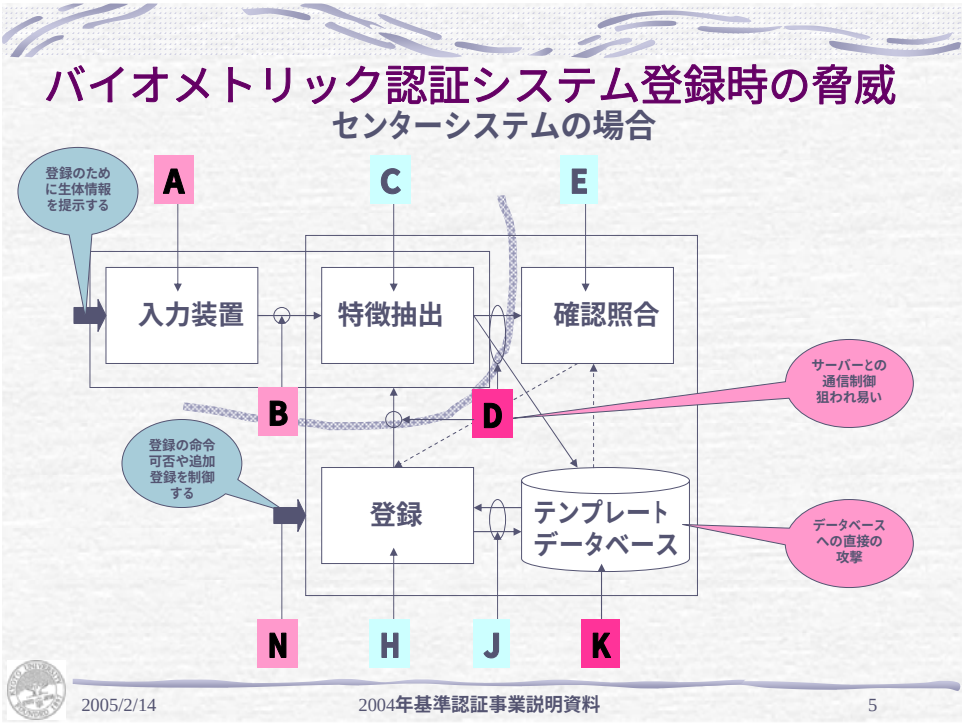


図　３－９　センターシステムの登録時脅威

センターシステムの場合は、入力装置および特徴抽出装置がローカルにあり、確認照合機能、登録機能およびテンプレート・データベースがセンターにある場合を想定している。バイオメトリクスデータは通信路により転送される。

従って、センターシステムにおいては、ローカルシステムの場合に加えて、「ローカルシステムとセンター間の通信路（通信制御）」Dポイント、「テンプレート・データベースへの直接の攻撃」Kポイント、「登録処理」Hポイント、テンプレート・データベースへの「アクセス通信路」Ｊポイントが脅威発生ポイントとして分析の対象となる。（図３－９　センターシステムの登録時脅威

参照）

D）Dポイント：ローカルシステムとセンターサーバ間の通信路
登録のために生体情報を転送する部位である。
発生する脅威としては、生体特徴情報（テンプレート）の不正変換があり、サーバとの通信制御が狙われ易い。

K）Kポイント：格納された生体情報のテンプレート・データベース
確認照合用に蓄積されたテンプレート・データベースに対する攻撃である。
発生する脅威としては、蓄積されたテンプレートの改竄がある。

H）Hポイント：システム装置内での登録処理
システム装置内での登録処理に対する攻撃である。
発生する脅威として、登録処理へのハードウェア・ソフトウェアのすり替えによる装置内部アルゴリズムのすり替えがある。

J）Jポイント：センターサーバ間の通信路
テンプレートのデータベースとサーバ間の転送部位である。
発生する脅威として、通信路における通信プロトコルのすり替えによるデータのすり替えがある。装置内部アルゴリズムのすり替えの脅威である。

3）センター管理の場合

クライアント・サーバ（センター管理）の場合は、入力機能および特徴抽出機能がクライアント側にあり、確認照合機能、登録機能およびテンプレート・データベースがサーバにある。センターシステムにも生体情報のテンプレート・データベースがあり、照合結果・登録可否などの情報のやり取りをサーバとセンター間の通信で行う。（図 3－10 クライアント・サーバ（センター管理））

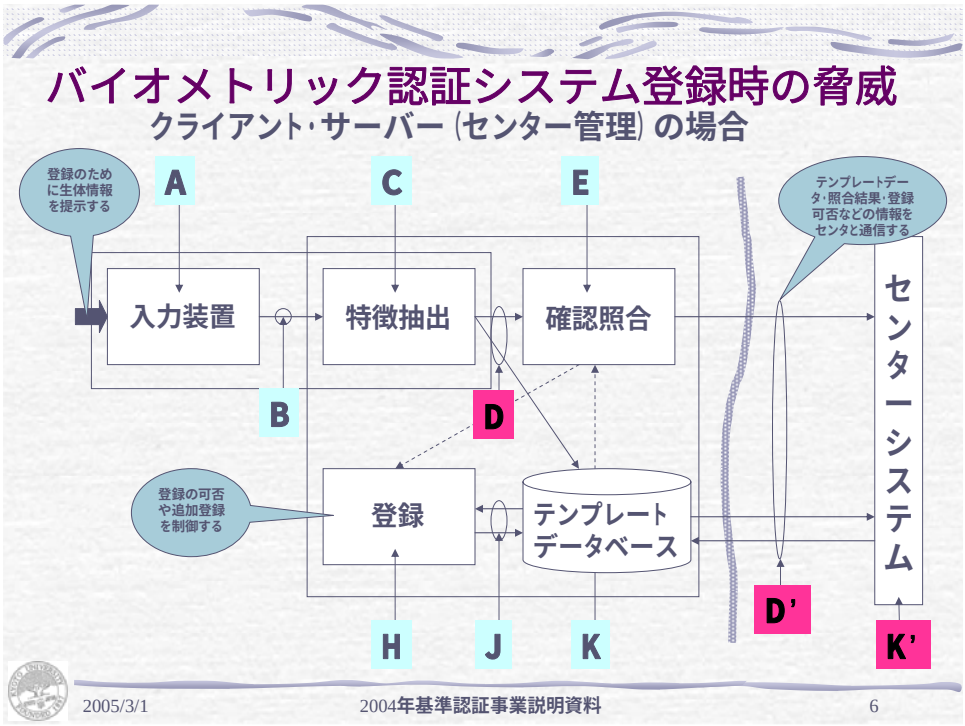


図　3−10 クライアント・サーバ（センター管理）

クライアント・サーバ（センター管理）の場合の脅威発生ポイントは、「クライアントとサーバ間の通信路」Dポイント、「サーバとセンターシステム間の通信路」D'ポイント、および「センターシステムのテンプレート・データベース」K'ポイントが分析対象となる。

D）Dポイント：クライアントとサーバ間の通信路
登録のために生体情報を転送する通信路である。
発生する脅威として、テンプレートの不正変換がある。クライアントとサーバとの通信制御が狙われ易い。

D'）D'ポイント：ローカルシステムとセンターサーバ間の通信路
登録のために生体情報を転送する部位である。
発生する脅威として、テンプレートの不正変換がある。ローカルシステムとサーバとの通信制御が狙われ易い。

K'）K'ポイント：センターサーバのテンプレート・データベース
センター管理の蓄積されたテンプレート・データベースへの攻撃部位である。
発生する脅威として、蓄積されたテンプレートの改竄がある。データベースへの直接攻撃によるテンプレートの改竄の脅威である。物理的なセキュリティが対応されている場合は、内部の管理者の人的問題が関与するケースが想定される。

（2）バイオメトリック認証システムデータ保存時の脅威

システム定常時（システムデータ保存時）およびアルゴリズム評価などシステムテスト時においても脅威の発生する可能性がある。下図はセンター管理システムの事例である。

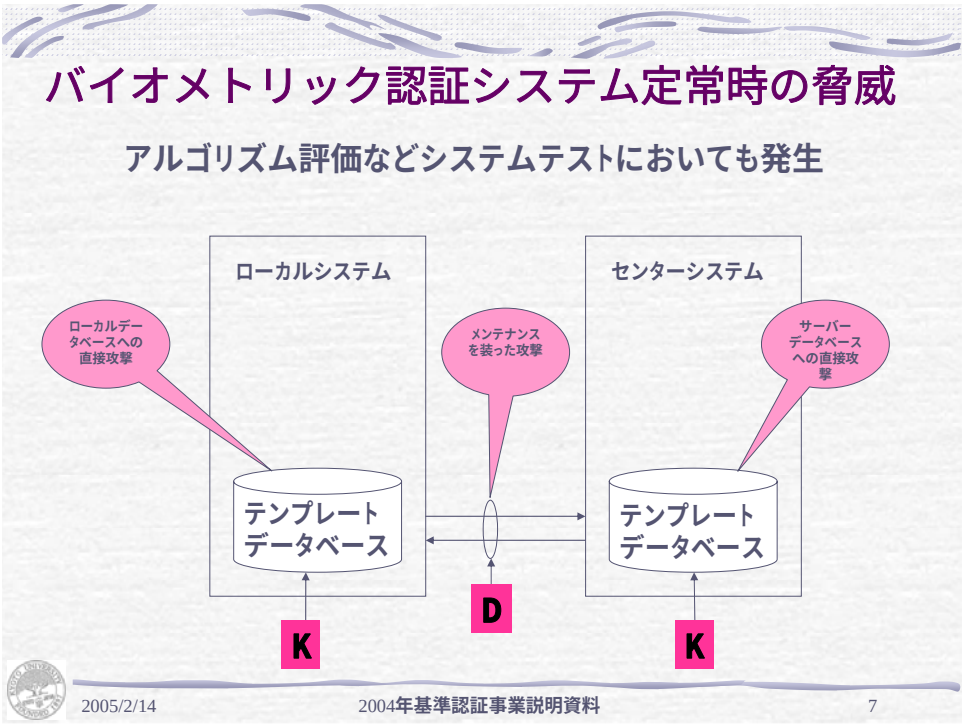


図　3 －11　システム定常時の脅威

この場合の脅威の発生するポイントとしては、「ローカルシステムおよびセンターシステムのテンプレート・データベース」Kポイント、「ローカルシステムとセンターシステム間の通信路」Dポイントがある。

K）Kポイント：ローカルシステム及びセンターシステムのテンプレート・データベース
登録・確認照合に蓄積されたデータが利用される。
発生する脅威として、蓄積されたテンプレートの改竄がある。データベースへの直接攻撃によるテンプレートの改竄・置き換えである。

D）ポイント：ローカルシステムとセンターサーバ間の通信路
登録・確認照合のために生体情報を転送する部位である。
発生する脅威として、テンプレートの不正変換がある。システムの保守を装った攻撃・通信プロトコルのすり替えによるテンプレートの変換・改竄である。

（3）システム運用時の脅威

システム運用時における、照合のための生体情報提示から、アプリケーションでのサービスが完結するまでの間に発生する可能性がある脅威について分析する。

1）ローカルシステム運用時の場合

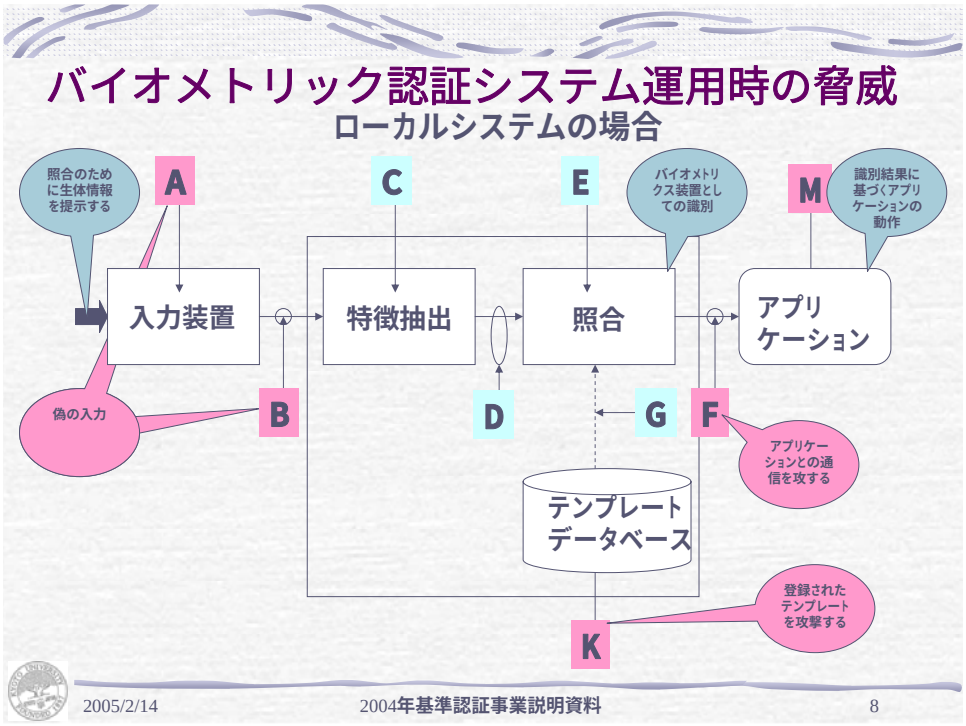


図　3 －12　ローカルシステム運用時の脅威

ローカルシステム運用時においては、入力装置における「照合のために生体情報を提示する」Aポイント、入力装置からローカルシステムへの「通信路」Bポイント、および「蓄積された生体情報のテンプレート・データベース」Kポイント、識別結果をアプリケーションシステムと通信する「ローカルシステムとアプリケーションシステム間の通信路」Fポイント、識別結果に基づくアプリケーション動作を実行する「アプリケーション」Mポイントが検討するべき脅威発生ポイントと考えられる。

Mポイントは、アプリケーションシステムに対する脅威であり、バイオメトリクス認証システムの範囲外なので、ここでの検討対象とはしない。

A）Aポイント：入力装置

照合のために生体情報を提示する部位

発生する脅威として、センサーへの偽の生体情報の提示がある。

B）Bポイント：情報通信路

照合のために生体情報を転送する部位。

発生する脅威として、蓄積された生体情報の再入力がある。偽情報による登録や照合の脅威である。

K）Kポイント：ローカルシステムのテンプレート・データベース
確認照合に蓄積されたデータが利用される部位。
発生する脅威として、蓄積されたテンプレートの改竄がある。登録されたテンプレートへの直接攻撃である。

F）Fポイント：ローカルシステムとアプリケーションシステム間の通信路
ローカルシステムとアプリケーションとの通信路である。
発生する脅威として、確認照合の最終判断のすり替えがある。通信路への浸入によりアプリケーションシステムへの照合結果をすり替えられる脅威である。

2）センターシステム運用時の場合

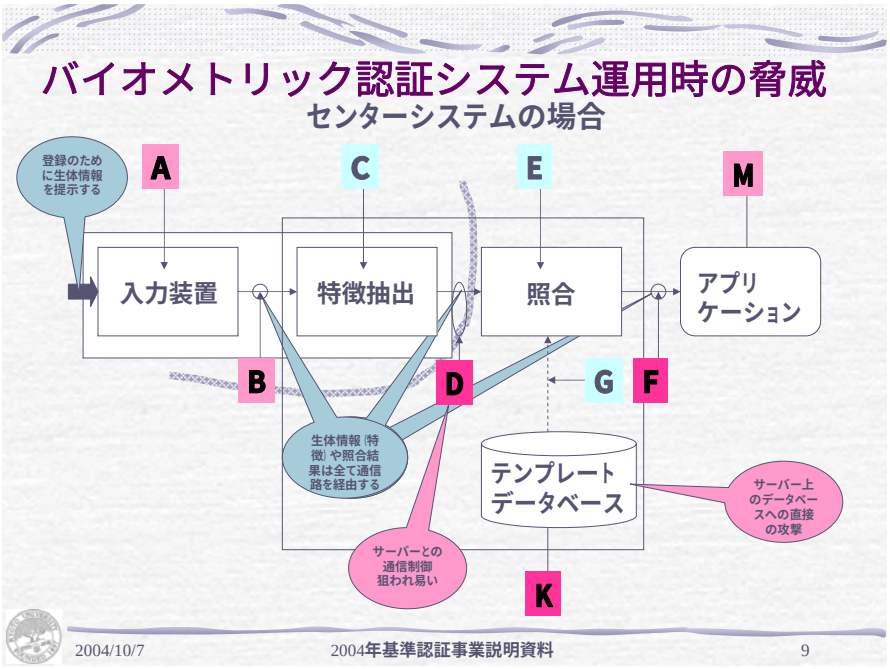


図　3 －13　センターシステム運用時の脅威

センターシステム運用時の脅威発生ポイントは、照合のために生体情報を提示する「入力装置」Aポイント、「入力装置と特徴抽出装置間の情報通信路」Bポイント、「特徴抽出装置センターサーバ間の情報通信路」Dポイント、「センターサーバとアプリケーションサーバ間の情報通信路」Fポイント、およびセンターサーバの「テンプレート・データベース」Kポイント、「テンプレート・データベースと照合装置間の情報通信路」Gポイントが想定される。

A）Aポイント：入力装置
照合のために生体情報を提示する部位である。
発生する脅威として、センサーへの偽の生体情報の提示がある。

B）Bポイント：入力装置と特徴抽出装置間の情報通信路
照合のために生体情報を転送する部位である。
発生する脅威としては、蓄積された生体情報の再入力がある。また生体情報が奪われる脅威がある。

D）Dポイント：特徴抽出装置とセンターサーバ間の情報通信路
登録・確認照合のために生体情報を転送する部位である。
発生する脅威：テンプレートの不正変換がある。サーバとの通信制御が狙われ易い。

F）Fポイント：センターサーバとアプリケーションシステム間の通信路
センターシステムとアプリケーションとの通信路である。
発生する脅威として、確認照合の最終判断のすり替えがある。

K）Kポイント：センターシステムのテンプレート・データベース
確認照合に蓄積されたデータが利用される。
発生する脅威として、蓄積されたテンプレートの改竄がある。
また登録されたテンプレートへの直接攻撃がある。

G）Gポイント：テンプレート・データベースと照合装置間の情報通信路
照合のためにテンプレートを参照する部位である。
発生する脅威として、蓄積されたテンプレートの改竄がある。通信路への浸入によりテンプレートを改竄する脅威である。

3）クライアント・サーバーシステム（センター管理）の場合
このシステム構成は、クライアント（入力・特徴抽出装置）、サーバ（照合・テンプレート・データベース）、センターシステム（照合結果・テンプレート管理がセンター）、アプリケーションシステムが情報通信路で接続されている。

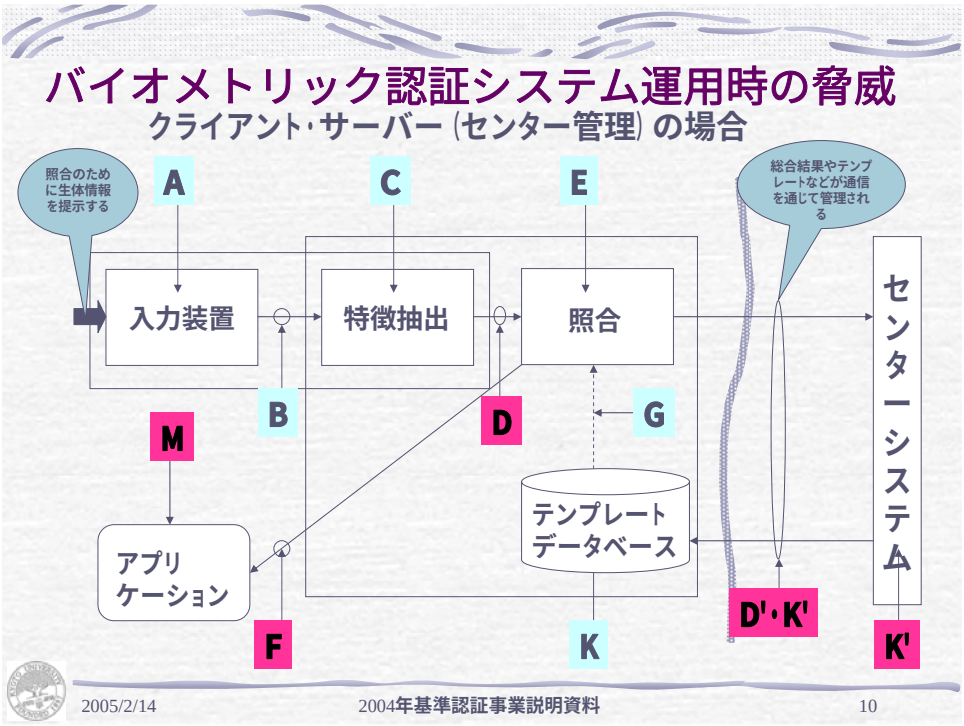


図　3 －14　クライアント・サーバ（センター管理）運用時の脅威

このシステムにおける脅威の発生ポイントは、「クライアントとサーバ間の情報通信路」Dポイント、「サーバとセンターシステム間の情報通信路」D'ポイント、「サーバとアプリケーション間の情報通信路」Ｆポイント、「センターシステムのテンプレート・データベース」K'ポイントが分析対象となる。

D）Dポイント：特徴抽出装置とセンターサーバ間の情報通信路
登録・確認照合のために生体情報を転送する部位。センター管理のため通信路となる。
発生する脅威として、生体特徴情報の不正変換がある。サーバとの通信制御が狙われ易い。

F）Ｆポイント：サーバとアプリケーションシステム間の通信路
サーバーシステムとアプリケーションとの通信路である。
発生する脅威として、確認照合の最終判断のすり替えがある。

K'）K'ポイント：センターシステムのテンプレート・データベース
確認照合に蓄積されたデータが利用される部位である。
発生する脅威として、蓄積されたテンプレートの改竄（登録されたテンプレートへの直接攻撃）がある。

（4）脅威分析の集約

ここまでに、バイオメトリック認証システムの「登録時」「定常時」「運用時」における脅威の発生する可能性があるポイントについて脅威分析を行った。これらの分析結果をまとめると表　3-3　脅威分析まとめ　になる。A，B、C等は、脅威発生ポイントを表している。

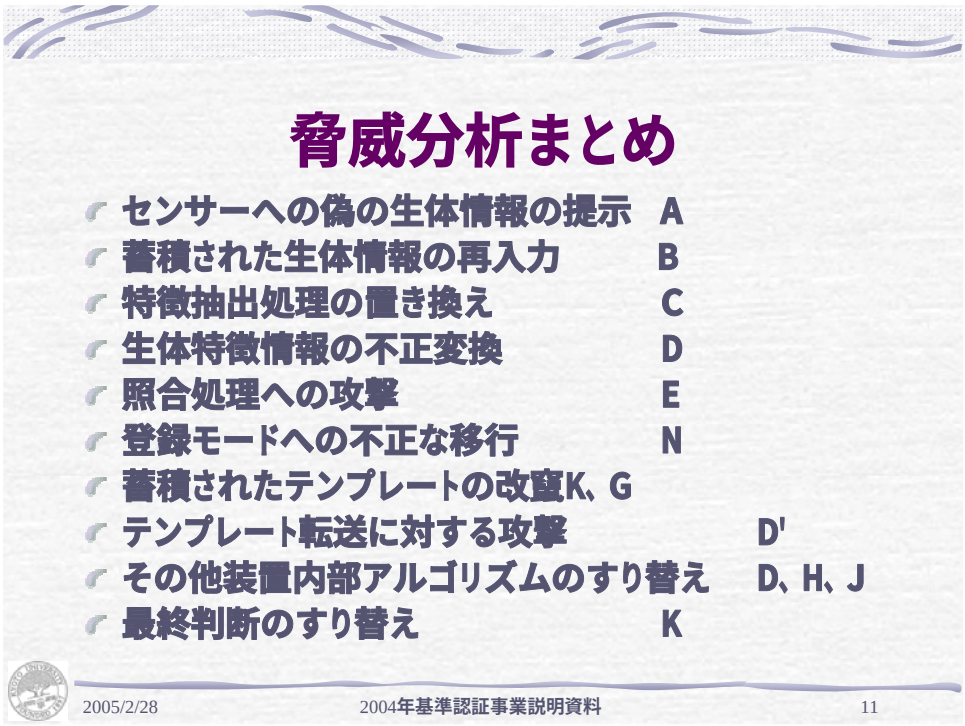


表　3−3　脅威分析まとめ

1）センサーへの偽の生体情報の提示　A

Aポイントにおいては、センサーへの偽の生体情報の提示という脅威が存在する。これらの脅威は、登録および定常時、運用時における確認照合において「なりすまし」につながる脅威である。なりすましにつながる脅威とは、第三者が利用者になりすまして認証を受ける攻撃や、個人照合において第三者が利用者として認証されてしまう事故などを指す。人工サンプルなどによるバイオメトリクス認証装置の詐称の脅威である。

2）蓄積された生体情報の再入力　B

Bポイントでは、入力装置と特徴抽出装置への転送路からの攻撃で、入力装置に残存したデータなどの蓄積された生体情報を、入力装置からの入力を装って再入力する脅威が発生する。

3）特徴抽出処理の置き換え　　C

Cポイントの脅威は、物理的もしくは特徴抽出ソフトウェアの置き換えにより、認証の真正性を破る脅威である。

4）生体特徴情報（テンプレート）の不正変換　　D

Dポイントでは、特徴抽出、確認照合、登録などのサーバ間の通信路において、テンプレート

を不正に変換される脅威である。

5）照合処理への攻撃　　E

Eポイントは、確認照合処理において、ソフトウェアの改竄や置き換えにより照合処理を攻撃する脅威が発生する。

6）登録モードへの不正な移行　　N

Nポイントでは、登録の命令可否や追加登録を外部から制御することにより、データを不正に登録してしまう脅威がある。

7）蓄積されたテンプレートの改竄　　K、G

K、Gポイントでは、データベースに蓄積されているテンプレートが改竄される脅威である。

8）テンプレート転送に対する攻撃　　D’

D’ポイントは、ローカルシステムとセンターサーバ間の通信路への攻撃により、センター管理の生体情報を不正に変換してローカルシステムの生体情報を不正なものとする脅威がある。テンプレートの生成ロジックが破られている場合に発生する。

9）その他装置内部アルゴリズムのすり替え　　D、H、J

D、H、Jポイントは、処理装置や通信路において、処理アルゴリズムやプロトコルなどのソフトウェアをすり替えることによりテンプレートをすり替えられる脅威がある。

１０）最終判断のすり替え　　K

Kポイントでは、通信路や通信制御装置においてアプリケーションに対しての最終判断がすり替えられる脅威が発生する。

３．２．４　バイオメトリクス個人認証システム運用時における情報の漏洩防止対策等、技術的可能性研究

バイオメトリクスに関する脆弱性情報の健全な流通の実現にむけて、脆弱性への対応方針の明確化、脆弱性情報の提供を促すための方策（ガイドライン策定）、脆弱性情報を受け付ける組織の整備などについての検討を行う。

（1）脅威対策

1）従来から提唱されている脅威対策

バイオメトリック認証システムにおける脅威分析で明らかになった各脅威ポイントにおける脅威に対する対策について検討する。

表3.2.2　脅威対策（1）に従来から提唱されている脅威対策の例が示されている。

（A）センサー部分(A)に対する脅威対策

センサー部分における脅威対策としては、本人確認のために、認証動作が不可解な者の検知等の「詐称検知」機能を備える対策がある。

「生体検出」機能により、人工サンプルによる攻撃に対応する。またセンサー面に、指紋等が残留しないような設計を考慮しておくことも必要である。

生の生体情報の漏洩を避けるためには、生体情報を保管せず、生体的特徴をテンプレートとして登録することも脅威のリスクを少なくする上で重要である。

（B）通信/伝送(B, D, F, G, J)に対する脅威対策

通信／伝送に対する脅威対策としては物理的に一体化した装置とすること、通信プロトコル、相互認証などのアクセス制御を隠蔽しておくことが必要である。

インターネットなどネットワークを利用してで安全に通信を行うためには、ＳＳＬ(Secure Sockets Layer)やＳＥＴ(Secure Electronic Transactions)、ＰＫＩ(Public Key Infrastructure)などによる「通信の暗号化」を計ることが必要になる。

ＰＫＩ（電子認証書）方式では、複数のセキュリティ対策が実現される。

- なりすましへの防御
- ＳＳＬ盗聴対策
- データ改竄
- センサー部やサーバのなりすまし防止
- アクセス制御や監査のための多くの情報を格納

（C）装置/データベース(C, E, H, K)：

装置／データベースについては、バイオメトリクス以外の個人情報と同じように、保管場所の安全管理が必要である。

また、装置間やデータの認証を行うプロトコルにより不正な装置やデータの浸入を排除することができる。

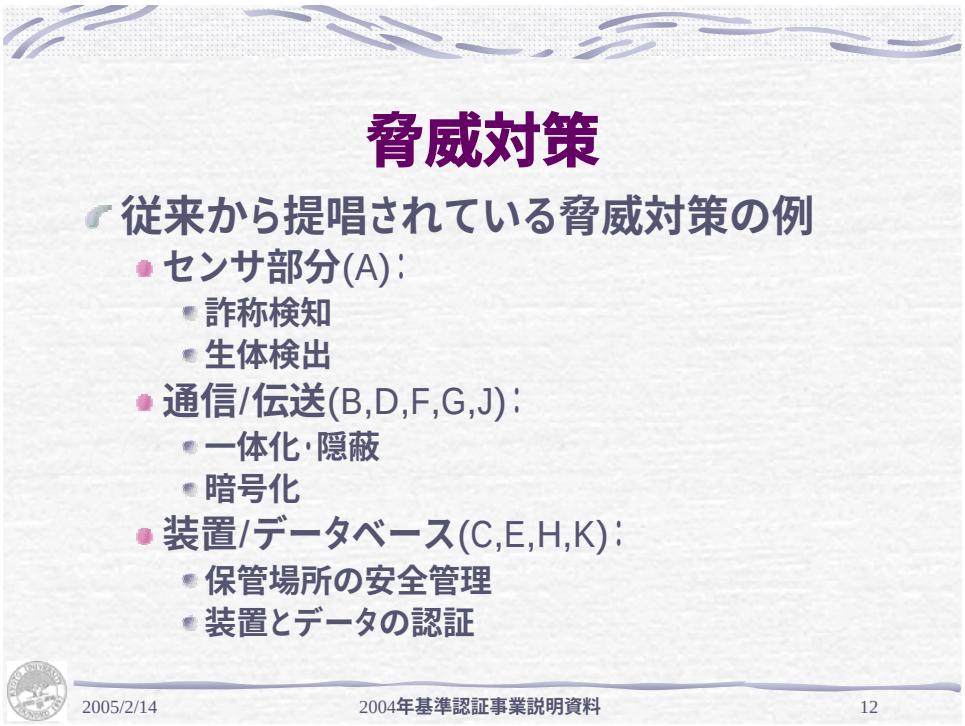


表　3－4　脅威対策の例

2）従来から提唱されている脅威対策の課題

○　センサー部分（A）：

「詐称検知」によるなりすましなどへの脅威対策は、詐称検知の原理が分かってしまえば詐称も可能になるという課題がある。

「生体検出」機能は、精度の高いものにすると、今のところの技術では、装置の大型化・コストアップが避けられない。

生の生体情報を保存しないで、個人認証をテンプレートで行うことにおいても、テンプレートが漏洩した場合には、問題が発生することが予想される。漏洩した場合にも被害の発生を防止出来るテンプレート保護技術が必要であり、防止技術の開発が大きな課題である。

○　通信/伝送（B, D, F, G, J）：

通信/伝送の一体化・隠蔽化については、リバースエンジニアリング手法によるプロトコルの復元が可能という脆弱性がある。

またＳＳＬ等による暗号化による脅威対策には、秘密鍵の管理（人的要因が絡む）という課題がある。

○　装置/データベース(C, E, H, K)：

装置/データベースについては、保管場所の安全管理が最終的には人的要因による問題を抱えている。

装置とデータの認証という脅威対策も、データセンターとシステムの運用、秘密鍵の管理という人的要因による脆弱性を有している。

○　個別の課題

センサー技術・暗号技術・運用技術の問題など、既存技術による対策に関連した課題はまだまだ多い。しかし、ここでは個々の抱える課題については取り上げない。

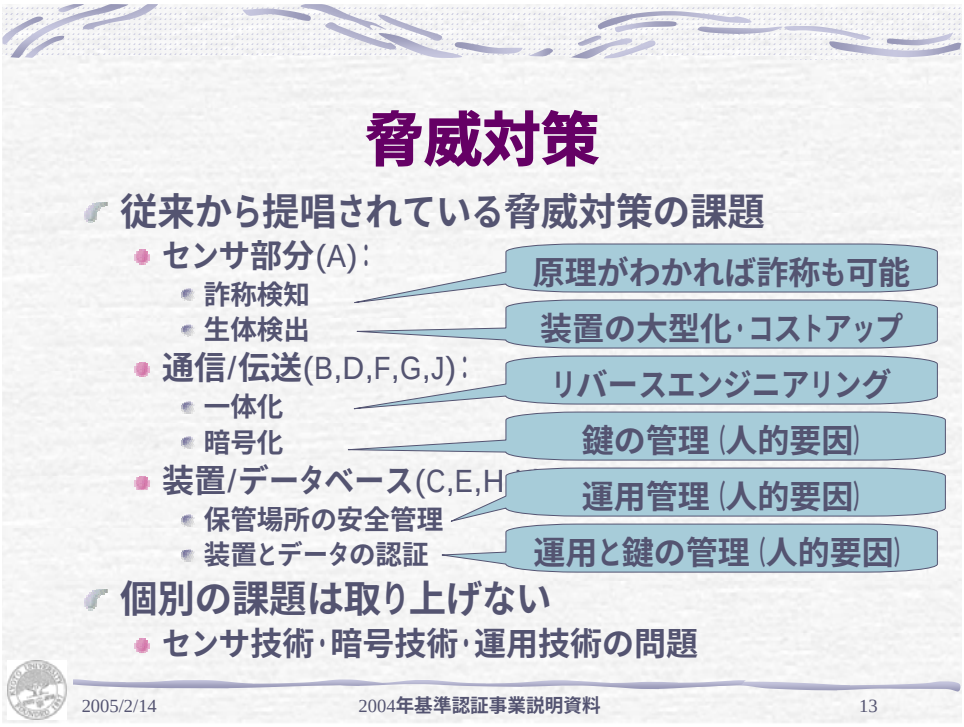


表　3−5　脅威対策の課題

（2）脅威対策のまとめ

従来から提唱されている脅威対策は、個々に問題点を抱えているが、それらをを厳密に実施することでシステムの安全性は向上する。個人情報や機密性の高いデータベースに対する既存のセキュリティ管理対策を、バイオメトリック認証システムにも適用することは有効である。

脅威対策を進める上で、考慮すべき検討課題としては、次のような点がある。

1．現実的な脅威対策の必要性

バイオメトリック認証システムに対する脅威対策は、コスト・小型化・スループット要求とのトレードオフになると想定される。発生するリスクを十分に評価して、適正な着地点を見つけることになる。当然ながら、個人情報の漏洩を避ける最低限の対策は、システムの設計方針として織り込まれなければならない。

一般的なセキュリティ対策と同じく、バイオメトリクスの脅威対策も人的要因を完全には排除できないことを検討に入れておく必要がある。

またあまり煩雑な手続きを伴う対策は、運用上実行されないという脆弱性を生むことになるので、運用性の観点からも対策を設計する必要がある。

2．脆弱性の高いポイントを明らかにする。

システムにおける脆弱の高いポイントを分析して、システム的対策をとるための設計指針を与えることも重要である。

3．アタックが一度でも成功した際の被害の低減化を目標とする。

生体情報は変更不可能なため、大変困難な課題である。しかしこれまでの研究によれば、次のような技術の開発により、防止技術の現実化が期待される。

☆　テンプレート保護技術

・悪意ある管理者であっても、テンプレートの取り出しや改竄を困難にする保護技術。

☆　テンプレート無効化技術

・略取されたテンプレートは無効化されて利用不可とする技術。

・不正に登録されたテンプレートは排除される技術。

☆　評価用データベース保護技術

・システム評価時に個人データを隠蔽する技術。

・評価などにおいて公開に耐えることができる個人情報を隠蔽する技術。

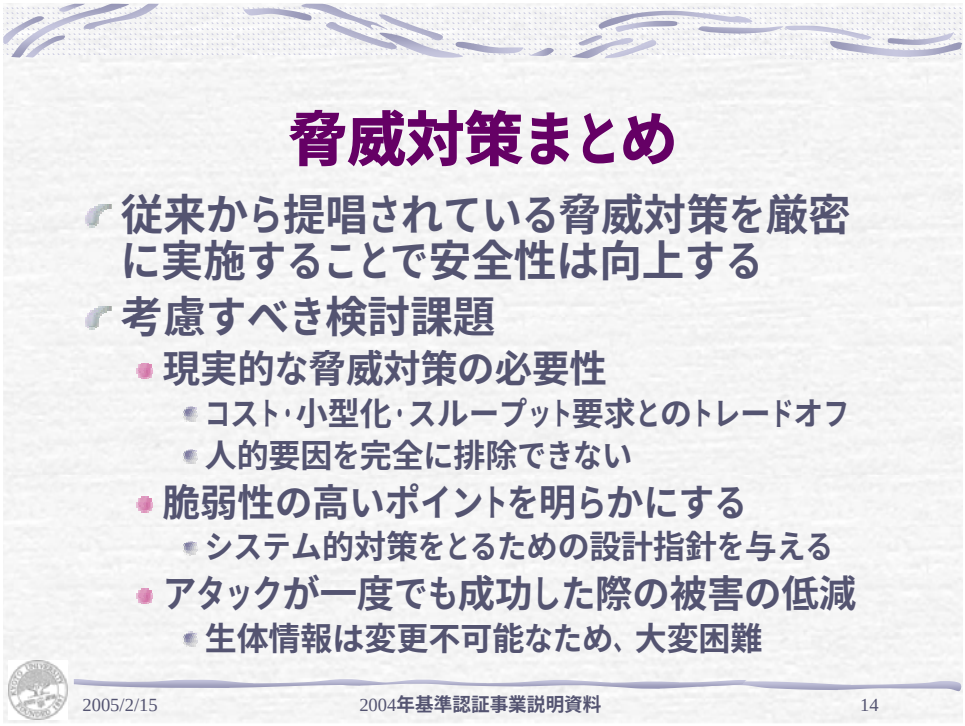


表　3−6　脅威対策まとめ

３．２．５　脅威対策の新技術開発の方向性

（1）新技術開発の方向性

バイオメトリクス認証は、本人の外見的な特徴や行動的特徴などの生体的特徴を利用して、あらかじめ登録された特徴のデータベース（テンプレート）との間でパターン間の類似性を評価して、あるレベルの類似性が確認されれば本人と認証する。そして、容易に人に教えたり貸し借りしたりできる秘密情報（パスワードや秘密鍵）や物証（身分証明書等）より安全であるとされて来たが、近年の研究によればバイオメトリクス個人認証に対して多くの潜在的危険性が指摘されるようになってきた。

バイオメトリクスデータの共通化、システム間での信用の継承も広がって来ており、国際標準化も進められている。バイオメトリクスデータの流通化と共通化のためのフォーマット標準化（ＳＣ３７-WG２/WG３/WG４）の活動がある。またデータ保護という観点から個人情報保護とプライバシーの問題（WG６）も検討されている。

バイオメトリクス個人認証においては、これまでの研究にもみられるように様々な脅威の発生が予測されているが、既存のセキュリティ対策を厳格に適用することにより、高い安全性を実現出来ることも想定されている。しかし、バイオメトリクスデータは漏洩してしまった際に取り替えることが出来ないという特徴から、テンプレートの保護技術がクリティカルな課題として研究されている。

こういった問題を解決するために、テンプレートを暗号化して保存したり、テンプレートと認証処理を、読み出し保護された可搬性メディア内部で行ったりする解決案も考えられている。しかしながら、これらの保護方式は小さな閉じたシステムでしか成り立たないものと思われる。

たとえば、電子パスポートのように、ある組織(国)で登録したテンプレートを任意の第三者に示して所有者を認証するようなアプリケーションにおいては、パスポートに保存されたテンプレートを読み出して、第三者が本人から取得した生のバイオメトリクスデータとテンプレートの間で同一性の認証を行うことになるが、登録システムと照合システムは同一とは限らないので、マルチベンダ環境で運用をサポートしなければならない。バイオメトリクスを取得するセンサーを含めた認証アルゴリズムの隠蔽は運用上不可能と言ってよく、そこでは、テンプレート自身を暴露された場合にも安全性を確保できるテンプレート保護技術がやはり必要となってくる。

テンプレートの保護には、悪意ある管理者であってもテンプレートの取り出しや改竄を困難化する技術と、奪われたテンプレートを無効化する技術や、不正に登録されたテンプレートを排除する技術などが必要とされてくる。

いったん登録したテンプレートを再登録によって無効化する技術、テンプレートから元のバイオメトリクスデータを復元したり、他の装置用のテンプレートに作り変えたりするなどの操作を不可能にする技術なども求められている。

以下、このようなテンプレートや個人データの保護技術について、運用中の個人認証テンプレートが盗まれた場合、および、システム評価用に蓄積された評価用データベースが盗まれた場合の二つの場合を想定し、それぞれの場合に、脅威を明らかにした上で、これまでに提案された技

術を調査し、今後解決するべき方策を明らかにする。

（2）テンプレートの脆弱性分析

テンプレート保護に着目して、脆弱性を分析する。バイオメトリクス認証のモデルは、図 3 －15 バイオメトリクス認証のモデル に示されている。このモデルは、指紋による例である。スキャナにより生のバイオメトリクスデータが取り込まれ、生体の特徴が抽出される。抽出された特徴は、特徴ベクトルのパターンとされて、既に登録さえているテンプレート（特徴ベクトル）とマッチングして認証を行う。

1）バイオメトリクスデータの漏洩個所

バイオメトリクスデータの漏洩個所としては、センサー部がある。残存した生体情報を写し取る、またトロイの木馬のような偽のセンサー装置を置き換えておくことにより生体情報を入手する、センサー信号を傍受して生体情報を盗むなどの方法により、生の生体情報を手に入れることができる。また、後で参照することを目的として、センサー部に保管されている生データのデータベースから盗まれる可能性もある。これらの生体情報を入手することにより、テンプレートを生成することが可能となる。

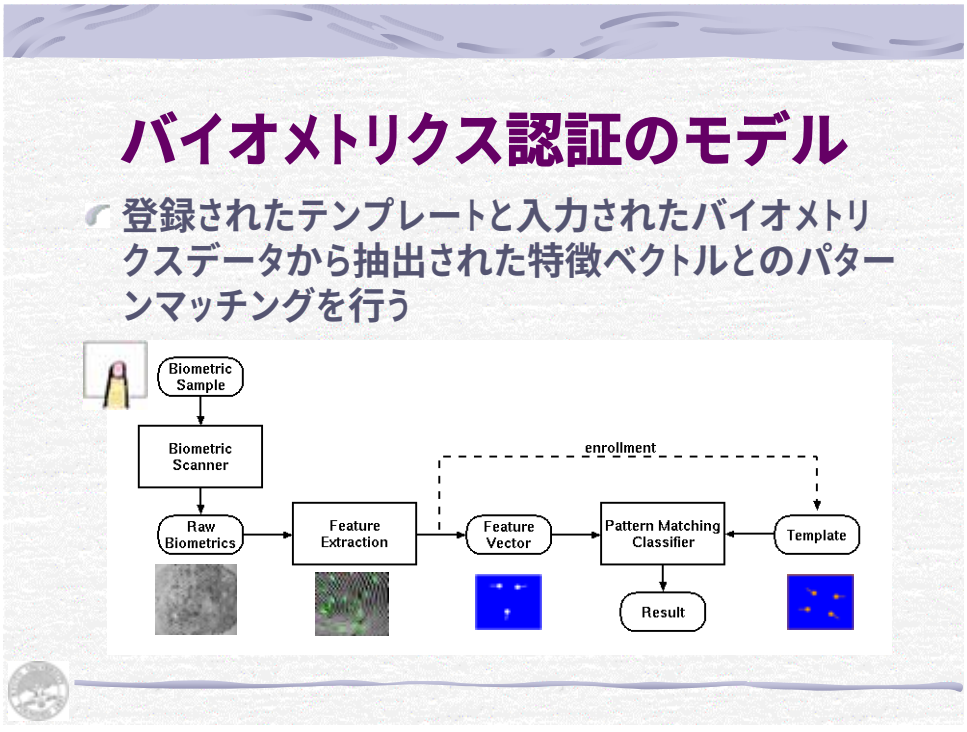


図　3 －15　バイオメトリクス認証のモデル

テンプレートの漏洩個所としては、センターのデータベースから盗み出す、センターと装置間の通信を傍受する、照合装置に転送・保管されたテンプレートを盗むなどがある。

また、集中保管されたテンプレートよりも、安全性が高いと考えられている、個人がＩＣカードなどにより携帯するいわゆる分散型のテンプレートには、媒体ごとテンプレートが盗まれる脆弱性

があることも認識しなければならない。

見過ごしてしまいがちな例としては、コンピュータのディスクに入ったデータが、廃棄されたコンピュータから漏洩することがあるのと同じように、放置・廃棄されたバイオメトリクス認証装置からデータが漏洩する危険性もあるので、注意する必要がある。またバイオメトリクス装置内で使用されているアルゴリズムの漏洩にも対策を考えなければならない。

具体的に、テンプレート漏洩のシナリオを見てみる。

A．テンプレート漏洩シナリオ（1）

図 3−16 テンプレート漏洩シナリオ（1）に示されるように、スキャナと認証システムの間に、生のバイオメトリクスデータが存在したり、テンプレートが個人認証システム内部に保存されていたりすると、傍受・盗難の可能性がある。

また、システムによっては、認証システム内に、目視確認のために生のバイオメトリクスデータを保存していることもあり、この場合も漏洩の危険がある。

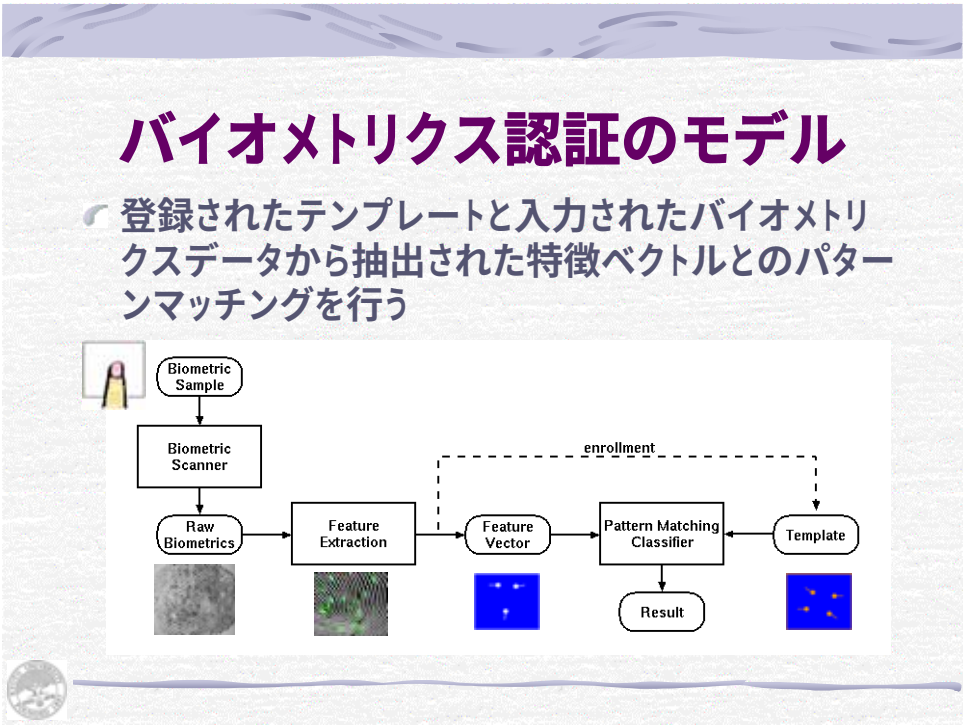


図 3 – 16 テンプレート漏洩シナリオ（1）

B．テンプレート漏洩シナリオ（2）

スキャナと照合装置が一体化されたスタンドアローンシステムやＩＣカードに暗号化したテンプレートを保存するシステムでは、テンプレートをセンター集中管理するシステムに比して、テンプレート漏洩に対する安全性が高まる。他方、媒体ごとテンプレートが盗まれる危険性は発生する。

しかしＩＣカードを用いてもシステムが暗号化したテンプレートを複合していると、複合さ

れたテンプレートが漏洩する可能性がある。暗号鍵が盗まれたり、機器内部のアルゴリズムが解析されたりするとテンプレートが復元可能となってしまう。

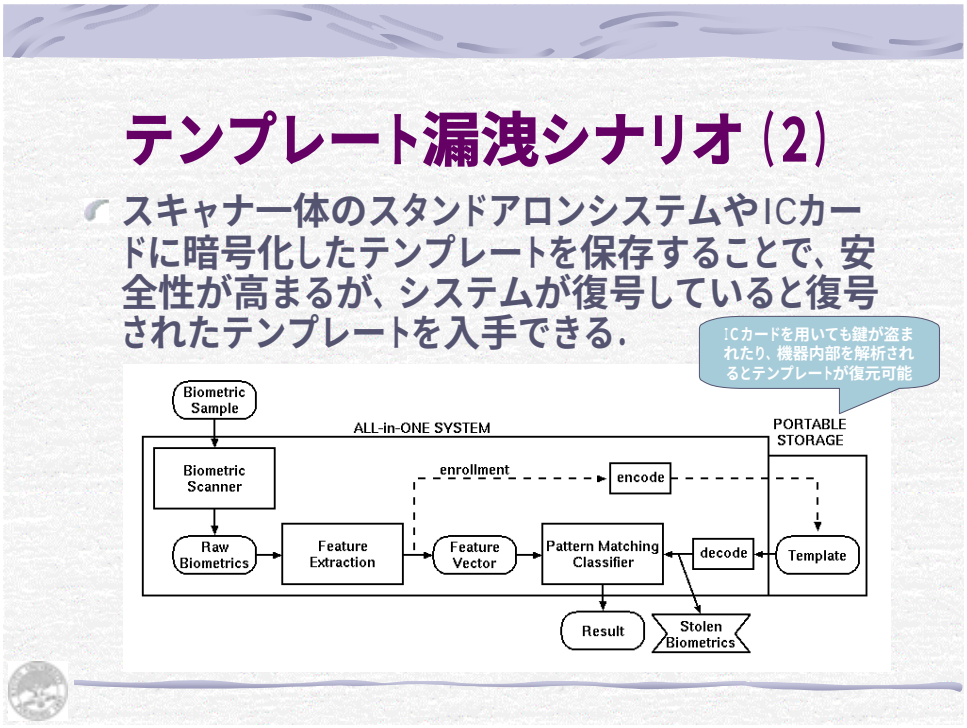


図　3 －17　テンプレート漏洩シナリオ（2）

C．テンプレート漏洩シナリオ（3）

今後世界レベルで普及が進むと予測されるパスポートの認証などに見られるテンプレートの相互運用可能なオープンシステムでは、テンプレートのフォーマットが公開されており、運用次第で容易にテンプレートを読み取ることができる。登録システムでモバイルメディアに保存されたテンプレートは、照合システムにおいて、本人の生バイオメトリクスデータから抽出されたテンプレート（特徴ベクトル）とパターン照合される。

電子パスポートなどのモバイルメディアからテンプレートが漏洩することが想定される。しかしながら、ＩＣＡＯ（国際民間航空機関）が策定するe-Passportにテンプレートの保護機能は検討されていない。

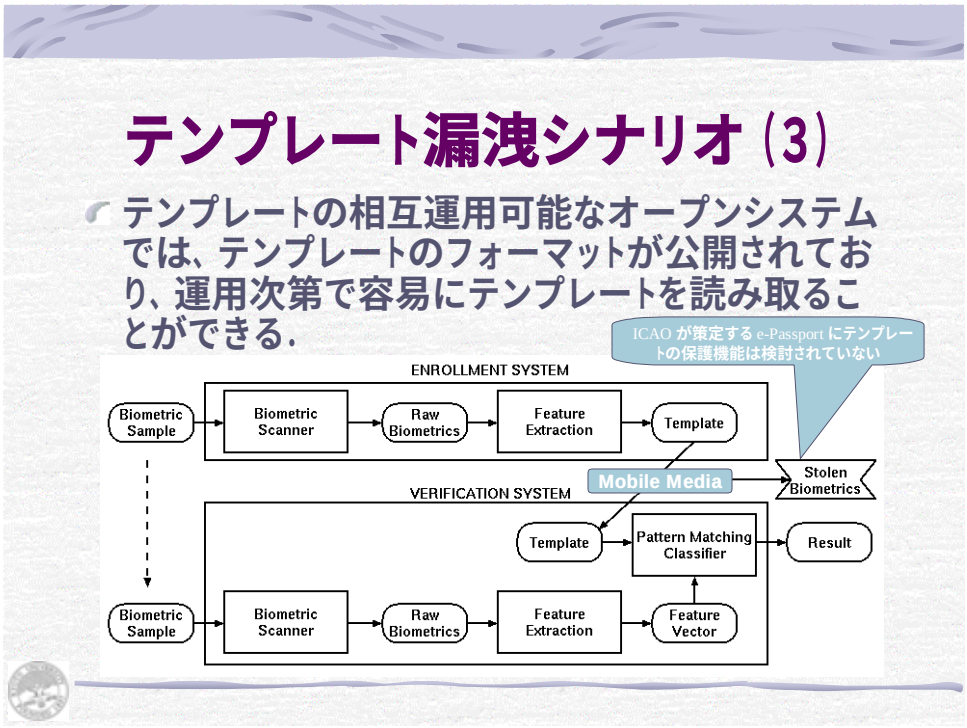


図　3 －18　テンプレート漏洩シナリオ（3）

2）テンプレートが漏洩した場合の危険性

生のバイオメトリクスデータを何らかの方法で入手して人工的に模擬したサンプルをつくることが可能であることは、これ迄の研究で指摘されていた。しかし、テンプレートが特徴ベクトルなどの生のバイオメトリクス情報ではなかった場合や、テンプレートから生のバイオメトリクス情報が直接復元不可能な形式であれば、テンプレートから生のバイオメトリクス情報は復元されないと考えられてきた。

それに対して、Hill は元の画像を含まないマニューシヤだけの指紋のテンプレートから認証可能な人工指パターンが生成可能なことを示し、 Adler は、主成分分析の固有画像への係数しか示されていない顔画像テンプレートから、同じテンプレートを生成でき認証に成功する顔画像を復元できることを示した。

従来、テンプレートは生のバイオメトリクス情報から特徴抽出処理を通して生成され、かつ、特徴抽出処理は画像情報から一部の有用な情報のみを抽出する変換であり、その逆変換は一意に決定できないことから、テンプレートから元のバイオメトリクス情報を復元することは不可能であるとされてきた。しかしAdler は、顔画像を例題にして、十分な大きさの顔画像データベースとアタックすべき目標のテンプレート、および、そのテンプレートと任意のバイオメトリクスサンプルとの間の照合率を得るアルゴリズムがあれば、元の顔画像を復元できることを示した。

（図 3 －19 攻撃ターゲットと山登り探索図　図 3 －21 元のバイオメトリクスデータ復元可能な条件 参照）

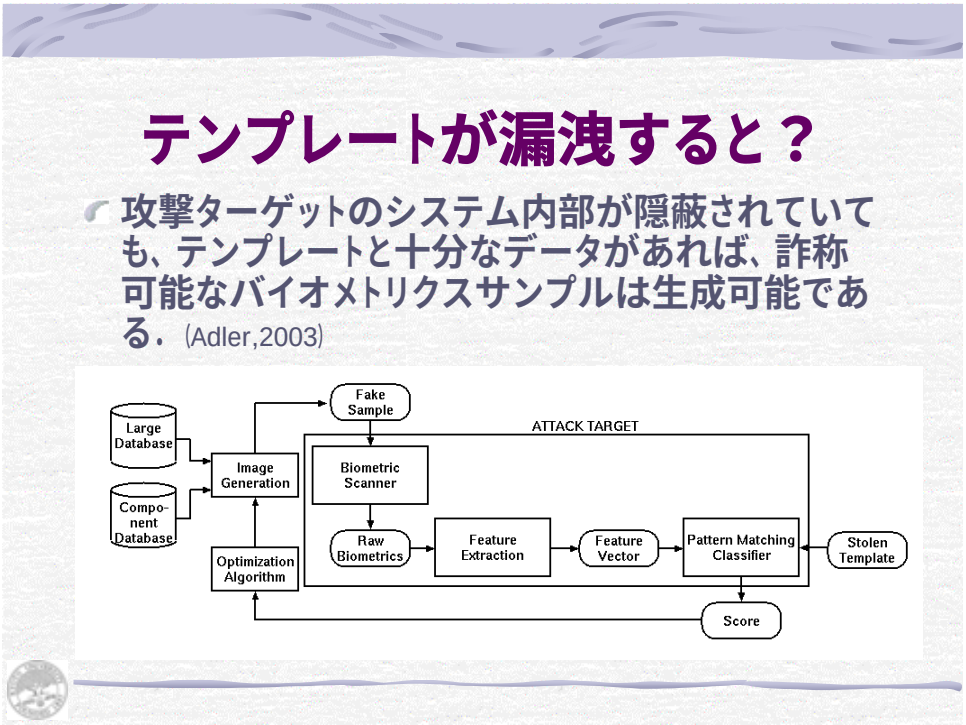


図　3 －19　攻撃ターゲットと山登り探索図

攻撃ターゲットのシステム内部がブラックボックス化されていて隠蔽されていてもテンプレートと十分なサンプルデータがあれば、詐称可能なバイオメトリクスサンプルは生成可能であることを Adler は示したことになる。

他人の顔を初期値として登録時者を詐称する顔画像を生成した例を示す。(Adler 2003　図 3 －20　顔画像推定の例　) 一番類似度の高い実在サンプルを初期値にして、特徴を構成する成分毎に類似度スコアを求め、山登り検索を行った。人が見ると合成されたことがわかるが、照合関数が返す距離は小さいので認証システムを詐称できる。

ほとんどのバイオメトリクス認証方式は、認証結果としてテンプレートとサンプルとの類似度（または距離）を出力するので、局所最適解につかまらないように十分な初期値を与えると最適化で認証可能サンプルを生成できる。 (図 3 －21　元のバイオメトリクスデータ復元可能な条件)

照合スコア関数の山が狭いと推定が困難になるので、推定を防止するためには、本当に類似度が高い時に山が高くなるような山の幅が狭い関数を使用しなければならない。しかし、実世界では個人の真のサンプルが毎日変動するので、許容量が少ないと、運用時に本人リジェクトを多発することになる。運用上は山を狭くすると問題が多くなり、また照合スコア関数の山が広いと、少ない初期サンプルから眞値が簡単に推定でき、脆弱性が高くなる。

頑健なシステムを作ると推定し易く危険な安全性が低いシステムとなり、実用性の高いシステムにしようとするとクリティカルなシステムになってしまう。

パターンマッチングで照合スコアによる相関関数を用いる方式をとる限り、こういったジレンマから逃れることは出来ないと言える。

図　3 －20　顔画像推定の例

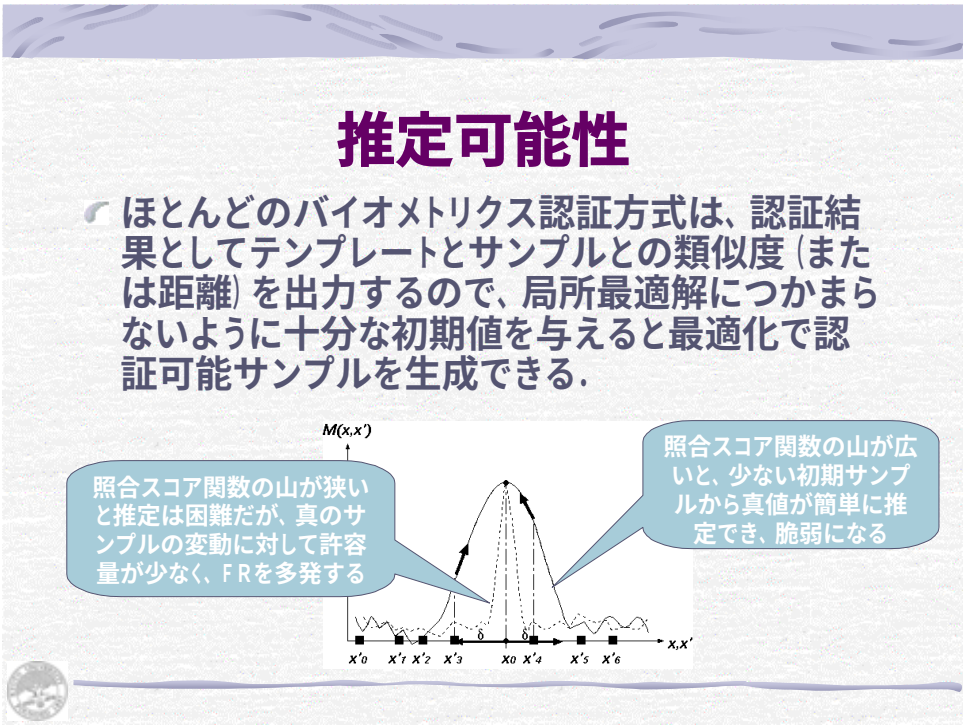


図 3 －21　元のバイオメトリクスデータ復元可能な条件

（3）テンプレート保護方式の研究･開発事例とその分析

これ迄述べたようなテンプレートの漏洩に対する安全性を強化するために、いくつかの手法が提案されている。テンプレートを暗号化して保管することもその一例ではあるが、認証機関の内部にも悪意ある管理者が存在する可能性を考えると、テンプレートの復号を前提としたシステムは安全とはいえない。そこで、本章ではオリジナルのテンプレートを必要としないバイオメトリクス認証システムについて研究開発の事例をサーベイする。

ここでサーベイするテンプレート保護方式は以下の３種類の方式である。

・Private template, cancelable biometrics方式

テンプレートは保護しないが、変形したテンプレートを用いてアプリケーション間での交換が不可であり、一旦発行したテンプレートを無効化可能とする方式である。

・Key hiding, key release方式

テンプレートを暗号化して保存しておき、照合時に復号して使用する。Hash 関数でエンコードされたテンプレートと入力サンプルが照合された場合にだけ、同様に保存された秘密鍵が取り出されて暗号を開けることができる。

入力画像のフーリエ変換位相項と二次元乱数から生成した復元フィルタと登録データでエンコードした秘密鍵とをテンプレートとする方式。

・Key generation, key binding

テンプレートと暗号鍵を一緒に暗号化しておき、照合された場合にだけテンプレートと組み合わされた暗号鍵が生成される。

1）Private Template, Cancelable Biometrics方式

Cancerable biometricsはIBMのRathaらによって提案されているテンプレート保護方法である。この手法は、バイオメトリクスデータを多対１の対応を持つ一方向 hash 関数によって変形させ、元のデータが復元できないようにする方式である。予測不可能な幾何学的変換を与えて、元のデータが復元できないようにするという概念を用いている。たとえば二次元のデータをブロックごとスクランブルして、複数のブロックから同じブロックへ特徴点を写像させると、元の特徴点配置は一意には復元不可能となる。あるいは、連続値関数の場合には、特定の関数を用いて変形させると、変換後の値 x から変換前の値 y を一意に復元不可能である。

Ratha はこの概念の具体的な実現方法として予測不可能な幾何学的変換を与えて、元のデータが復元できないようにすることを提案した。図 3 －22 に示す変換では、ブロック単位で位置を入れ替えることにより元のテンプレートを予測することが困難になっている。この手法は離散的に存在する特徴点のテンプレートを保護するのに適している。また、図 3 －23 の変換では、ブロックの形状に幾何的歪みが加えられ、それに合わせて元の図形を歪ませている。この手法モーフィング は、ブロック境界での連続性が保存されるので画像のテンプレートを保護するのに適している。

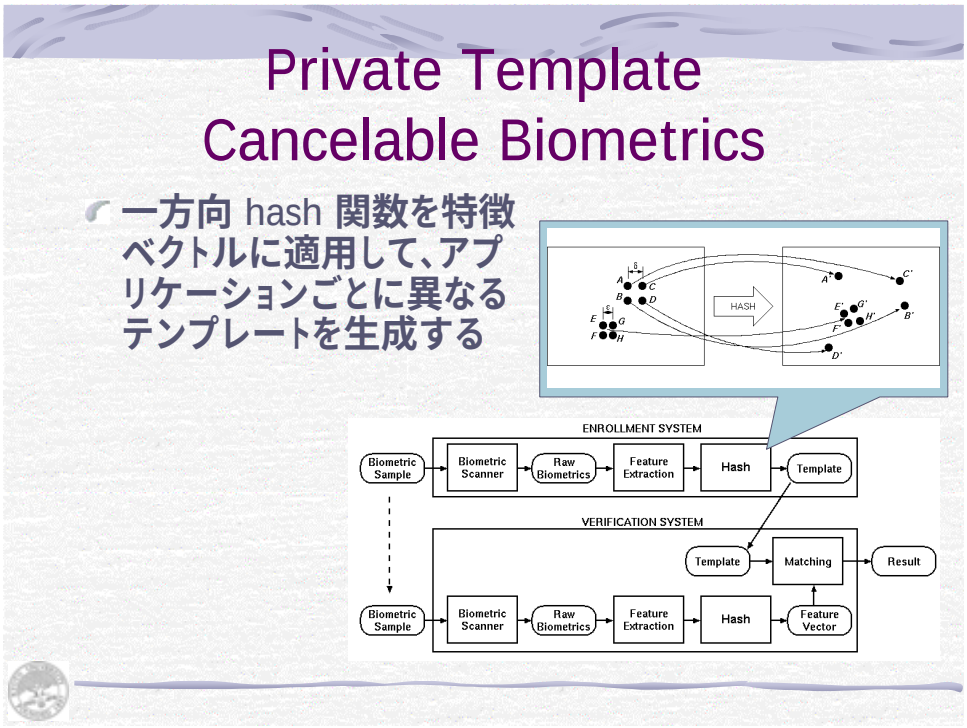


図 3 −22　Private Template, Cancelable Biometrics

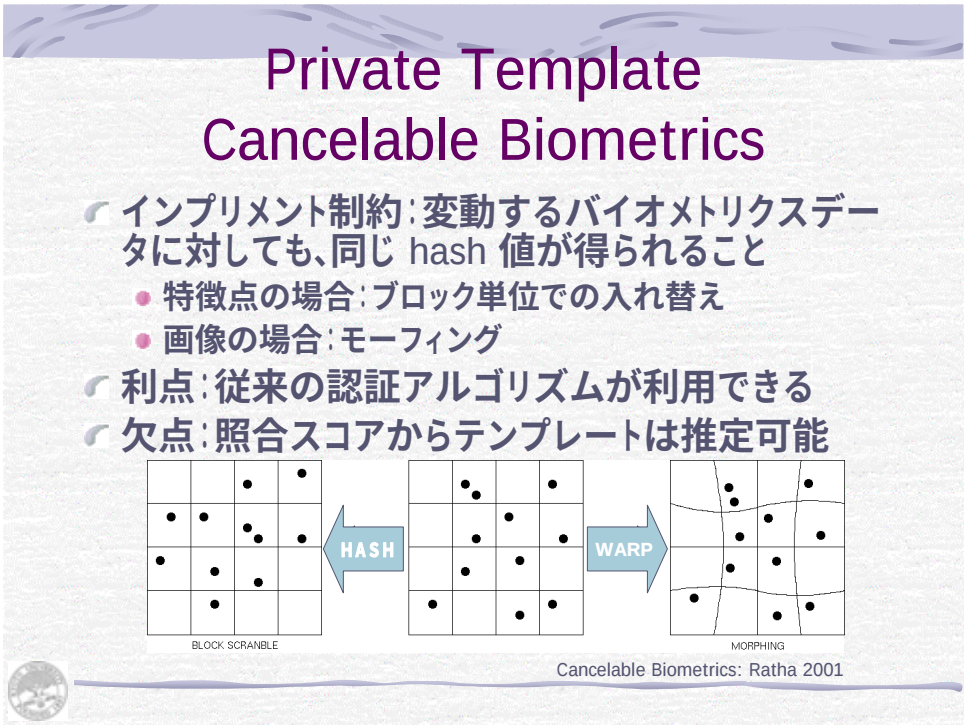


図3 −23　Private Template, Cancelable Biometrics

この方式の優れた点は保護後のテンプレートの形式やデータの意味がテンプレート保護を行わない従来のテンプレートと互換性が高い点である。そのため、特徴抽出やマッチングのアルゴリズムがそのまま利用でき、プライバシー保護されたテンプレートへの移行がスムーズに行える

という運用上のメリットが大きい。実用的には推奨出来る方式といえる。

さらに、従来型のマッチングに於いては、類似度が連続値で得られる場合が多く、その場合、たとえ直接元のテンプレートが復元できなくても、ほどほどに良いテンプレートを初期値として探索し、そこから山登り探索を行えば、他人になり済ますことのできるテンプレートを生成可能であるという危険性は残ったままである。照合スコアからテンプレートは推定可能という欠点があるが、技術発展過程における過度期の技術としては評価できる。

まとめると以下のようになる。

○一方向 hash 関数を特徴ベクトルに適用して、アプリケーション毎に異なるテンプレートを生成する方式。

○インプリメント制約:変動するバイオメトリクスデータに対しても、同じ hash 値が得られること

・特徴点の場合：ブロック単位での入れ替え

・画像の場合：モーフィング（変形を加える）

○利点：従来の認証アルゴリズムが利用できる

○欠点：照合スコアからテンプレートは推定可能

2）Key Hiding, Key Release方式

Cancerable biometrics のような一方向 hash 関数は使うが、特徴抽出やマッチングのアルゴリズムに互換性を持たせた方式とは異なり、暗号理論を用いてテンプレートを保護するとともに、入力画像の揺らぎを helperdata により訂正する機能を与えたものが考案された。

Hash 関数でエンコードされたテンプレートと入力サンプルから生成されたテンプレートが一致したときにのみ、秘密鍵がデコードされて取り出せる。照合率が出てこない方式なので、山登り探索を防止できるので安全性が高い方式である。

実装の例として１９９８年にカナダのバイオスクリプト社が光ニューロコンピュータを使って行った例が報告され、その後デジタル信号処理による実装方法も示された。

図 3 －24 にこの方式の登録過程と照合過程を示す。図 3－25 において登録時の入力サンプルデータはXi(i＝1,…,*N*)である。それぞれの入力サンプルは、フーリエ変換によって周波数空間での表現に変換され、入力信号と全く無相関の信号Ｓを畳み込むことによって、ＸをH（u)やCoから推測することは不可能にしている。

この方式でテンプレート・データベースに保存されるデータは、フーリエ変換した入力サンプルの虚数部の平均パターンにランダムなビットパターンを畳み込んで得られたフィルタ*関数*、畳み込み結果をフーリエ逆変換して閾値処理した二次元二値ビットマップにランダムなキーを適用して得られるルックアップテーブルのハッシュ値だけであり、これらの値から生のバイオメトリクスデータxiや、その成分を復元することができないという復元困難性が得られる。テンプレート・データベースが漏洩した場合には、パラメータを変更することで、新しいテンプレートを生成でき、漏洩したテンプレートを無効化することができる。無効化したテンプレートと新しいテンプレートとはビットパターンと秘密鍵が無相関であるため一方から他方を推定することができないという安

全性が保証されている。

この方式では、入力画像のフーリエ変換位相項と二次元乱数から生成した復元フィルターと登録データでエンコードした秘密鍵をテンプレートとしている。

利点としては、フーリエ関数を使用しているので、サンプルデータの位置ずれの許容度が大きいこと、盗まれたテンプレートの無効化が可能なことがある。

欠点としては、たくさんのデータを使うと Hash 関数を推定することから秘密鍵の生成ロジックを推定することの可能性がある。

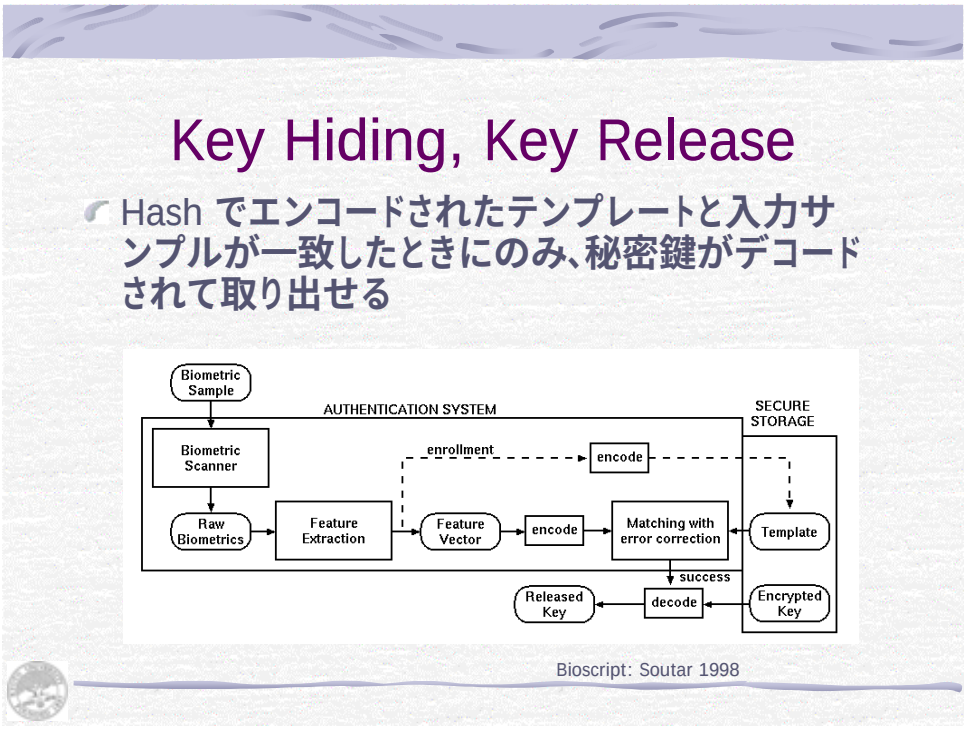


図 3 −24 Key Hiding, Key Release 1

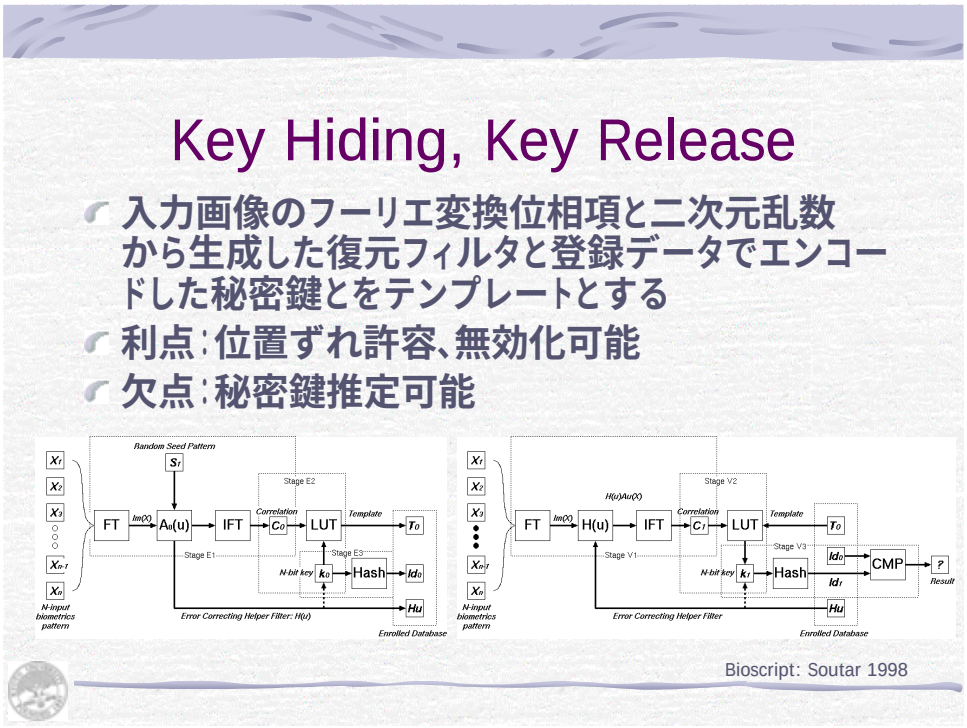


図　3 －25　Key Hiding, Key Release２

3）Key Generation, Key Binding 方式

この方式は、入力サンプルをエンコードし、一方向 Hash 関数によって復元不可能なテンプレートと入力データの揺らぎを補正する働きをもつ Helper Data とをテンプレートに持って、認証成功時に毎回同じ鍵を生成する。単純な Hash 関数が入力データの揺らぎによって、全く違う位置に写像してしまうのを、Helper Dataによってエラー訂正を行う考え方である。

この方式に類別される多くの提案は、暗号の専門家による理論的な提案であり、実証された方式では無かったが、表 3－7　Key Generation, Key Bindingの実証　にあるように、２００３年に Fingerprint Vault という具体的な実装方法が示された。この方式は、個別のバイオメトリクスに対する具体的な実装方法を示したという点で評価できるが、表 3－7 の他の方式同様、あらかじめ位置合わせが必要という欠点を持っている。位置合わせには暗号化されていないテンプレートが必要であり、このテンプレートから個人のバイオメトリクスデータの概略が類推できてしまう可能性が残っている。またテンプレートそのものの安全性は高いが、実世界で生じる同一人物のバイオメトリクスデータの変動に対する許容範囲の広さに難点があるものが多い。

Fingerprint Vault　方式は、真の特徴点 と偽の特徴点（chaff）とをテンプレートに登録し、入力サンプルの特徴点（赤）との一致不一致のコードを復号キーとして用いる。あらかじめ定められた近傍内に特徴点が発生すれば、少々位置がずれていても一致したと判別することにより、微小位置変動は吸収できる。また、この近傍の大きさを、個人の特徴点が日常の取得操作によって変動する範囲を統計的に計測し、その大きさに合わせて設定することによって、個人内変動を許容しつつ他人に対する識別性能を最大化することを提案している。また、個人内変動による特徴点の余分な発生と消滅については、エラー訂正を行うことを提案している。

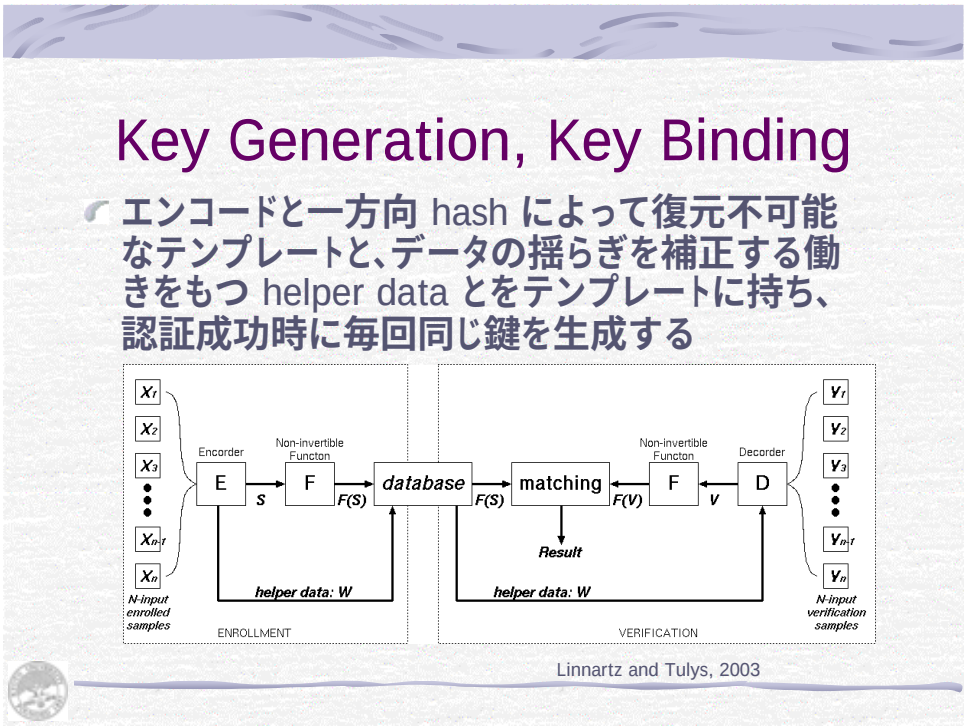


図 3 －26　Key Generation方式の基本アーキテクチャー

しかし、他の提案と同じく、個人内の変動範囲まで概略位置合わせがあらかじめ完了していなければならず、かつ、エラー訂正で補償可能な程度の少ない特徴点の発生・消滅しか許容していないところが、実用上の課題とされている。

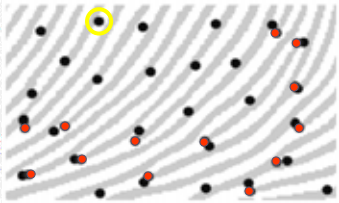
Key Generation, Key Binding

方式·筆者·発表年	適用対象	位置合わせ	変動許容	安全性
Shielding Function, Linnartz, 2003	Theory only	×	×	△
Fuzzy commitment, Juels, 1999	Theory only	×	×	○
Fuzzy vault, Juels, 2002	Theory only	×	×	○
Fingerprint vault, Clancy, 2003	Fingerprint (minutiae)	×	△	○

表3－7 Key Generation, Key Bindingの実証

Fingerprint Vault

- 真の特徴点と偽の特徴点（chaff）とをテンプレートに登録、入力サンプルの特徴点（赤）との一致不一致のコードを復号キーとして用いる
- 利点：微小位置変動は従来の特徴点照合と同じアルゴリズムで吸収可能
- 欠点：事前の概略位置合わせ必要



Clancy et al., 2003

図3 －27 Fingerprint Vault

4）これまでの研究の分析

これまでの研究をサーベイしてきたが、問題点をまとめてみると以下のようになる。

◎雑音に頑健な方式は、安全性が不完全である。

方式：Private template, Cancelable biometrics

◎ほどほど頑健だが、究極の攻撃に不完全である。

方式：Key hiding, Bioscript,

◎暗号理論的な方式は、現実の大きな雑音下では本人拒否を多発することが予想される。

方式：Shielding function, Fuzzy commitment, Fuzzy vault, …

このように、どの研究も強さと弱さを併せ持っているのが現状である。

課題としては、認識対認証のジレンマの問題が考えられる。パターン認識は、ほどほどの類似の許容が前提になり、認証は、完全な一致が要求される。生体情報のパターン認識と、１００パーセントの認証目標を包含しているバイオメトリクス個人認証は、どこかで現実的な決着点を見つけることができる技術を求めていると言えよう。

もう一つの課題として、雑音耐性と安全性は背反するという問題がある。

- 姿勢（並進・回転最大6自由度）、変形（非剛体弾性ひずみ）の補正には探索が必要であるが、探索を可能にすると、適当な初期値から真値の推定を可能にする。
- 信号の欠落、部分隠蔽、装飾などの誤りを訂正する能力は、本来拒否すべき入力を受け入れやすくする。

（4）テンプレート保護に関して今後開発すべき技術の提案

これまでのテンプレート保護に関する技術についてのサーベイから、今後開発するべき技術の提案をまとめてみる。

１．テンプレート保護に適した認証アルゴリズムの提案

- 位置合わせと照合との分離・独立
- 個人内変動と個人間変動の分離・独立
- 位置合わせ、個人内変動のモデル化と補償
- 類似度（距離）カーブがシャープな照合関数
- 位置合わせ+個人変動補償、照合を独立に行う two-stage アルゴリズムが有効

２．個別バイオメトリクスごとの実装方式開発

テンプレートを保護方式には、

１．Distortion transform：近傍での距離が保存され、遠方での距離が大きく変化する幾何的な変形を与える方式

２．Hashing with helper data：微少な変動に対するエラー訂正コードを導入した上で、一方向ハッシュ関数を適用する。

という二つの方向がある。

前者は、従来の特徴抽出や照合処理との互換性が高く、システムの移行の障壁が低いので、既存の中・小規模バイオメトリクス個人認証システムをアップグレードするために利用するには適しているが、テンプレートの秘匿の性能の点では十分ではなく、照合関数の仕様が公開されていたり、不特定多数の認証機関へ配布するような用途では安全とは言えない。

後者は、エラー訂正される範囲パラメータと、識別可能距離とのパラメータを指定して、識別性能を作り込むことが可能であり、広範囲に利用できることが予想されるが、現実の運用に当たっては以下のような課題が残っている。

・入力雑音モデルの推定
・雑音モデルと識別性能要求の矛盾
・複合バイオメトリクスへの拡張困難性

これまでの技術を検討して以上のような課題が判明したので、現在次のような改善を行うことを検討している。

1．過去のデータベースから入力雑音モデルをオフラインで推定し、登録時の個人サンプルから得られる雑音モデルの不完全さを補う。
2．雑音モデルの要因別ヘルパーデータの設計と実装。

特に、特徴点の座標や特徴点の属性を用いたマッチングに対して、適切な雑音モデルを立てて、それに応じたヘルパーデータ／エラー訂正をインプリメントすることで、識別性能とノイズ耐性との両立が見込めるであろう。

以上、テンプレートの脆弱性解析を行い、テンプレート保護の要求は社会的に高まっていること、脆弱なシステムの氾濫は社会の混乱を招く恐れが高いことを指摘した。

次に、テンプレート保護技術の調査・分析を行い、主要な技術として、(1) Private template, Cancelable template、 (2)Key hiding, Key retrieval, (3)Key generation, Key binding の三方式を紹介した。現状では十分実用的な実装は存在せず、問題点の指摘と今後の方策として、保護（照合関数のシャープな）に適したtwo-stage アルゴリズムの必要性を述べた。

（5）評価用データベース保護技術

評価用データベースにはバイオメトリクスデータ以外の個人情報は含まれないのでデータが漏洩したり不用意に公開されたりすることによる被害は少ないのではないかと考えられがちであるが、実際には以下のような危険性が存在する。ここでは、バイオメトリクスのアルゴリズム評価に用いられる　図 3 －28　に示すモデルによって、評価用データベースに存在する脅威を分析する。われわれの分析によれば、評価用データベースに存在する脅威は下記の三通りに分類できる。

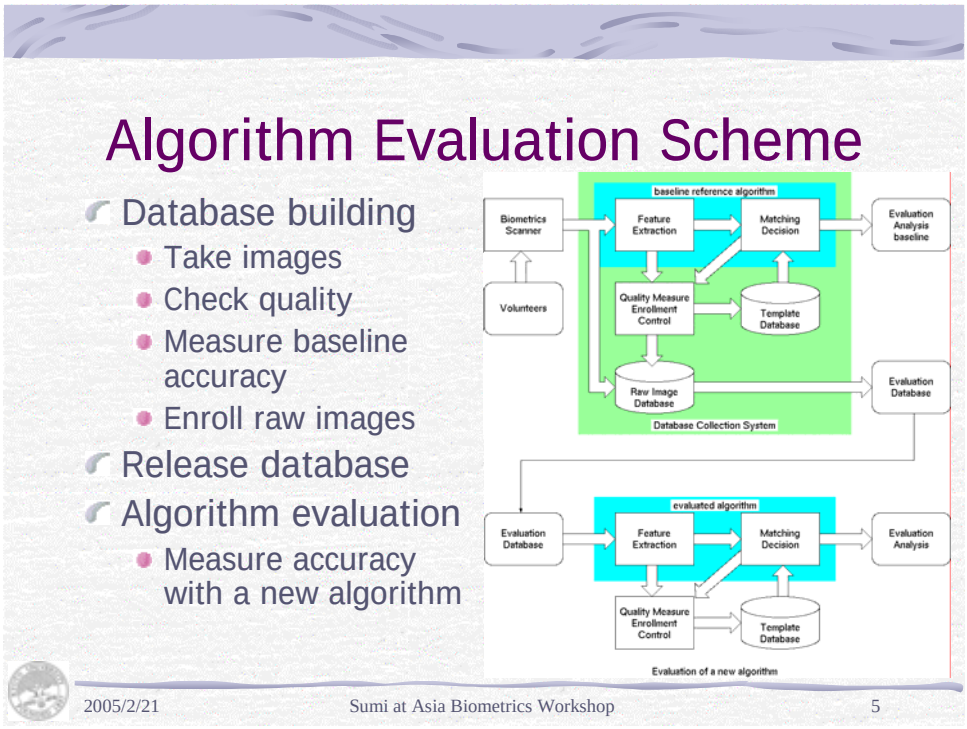


図3 －28　バイオメトリクス個人認証における評価モデル

（本人データの盗みだし）もし、被験者がデータベースに固有の識別番号がつけられていたり（二重登録されることを防ぐために何らかの固有識別番号が必要である）、 また、 マルチモーダルバイオメトリクス評価のために顔画像と組み合わせて登録されたりしていると、簡単に個人を特定できてしまう。そのため、データベースに登録された人物のデータを盗み出して、そのバイオメトリクスデータを偽造して本人になりすますという可能性がある。（ 図 3 －29　本人データの盗み出しの発生ケース１）

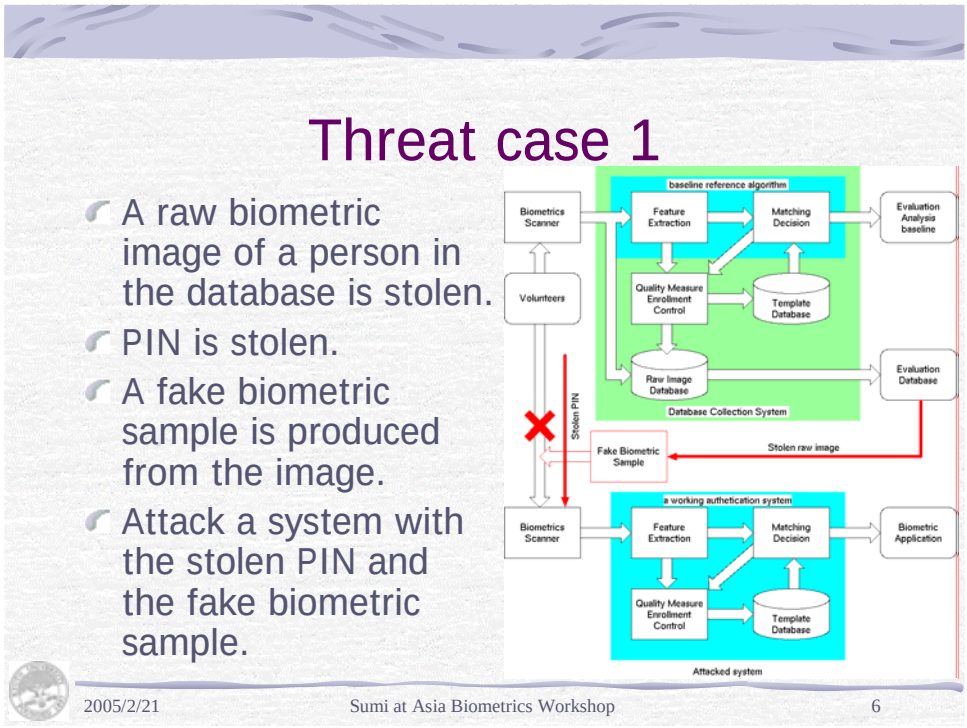


図3 －29　本人データの盗み出しの発生ケース１

（瓜二つの人物の抽出）データベースとは無関係の個人の権限を奪い取るために、まず攻撃対象の個人のバイオメトリクスデータを何らかの方法で盗み出す。次に、規模の大きな評価用バイオメトリクスデータベースから最も良く似た人物を選びだし、該当する被験者を説得または脅迫して、攻撃対象の人物に成り済まさせるという可能性がある。この場合、生身の人間を使うので、バイオメトリクス認証装置が生体検知機能を持っていたとしても詐称することが可能になる。（ 図 3 －30 ）

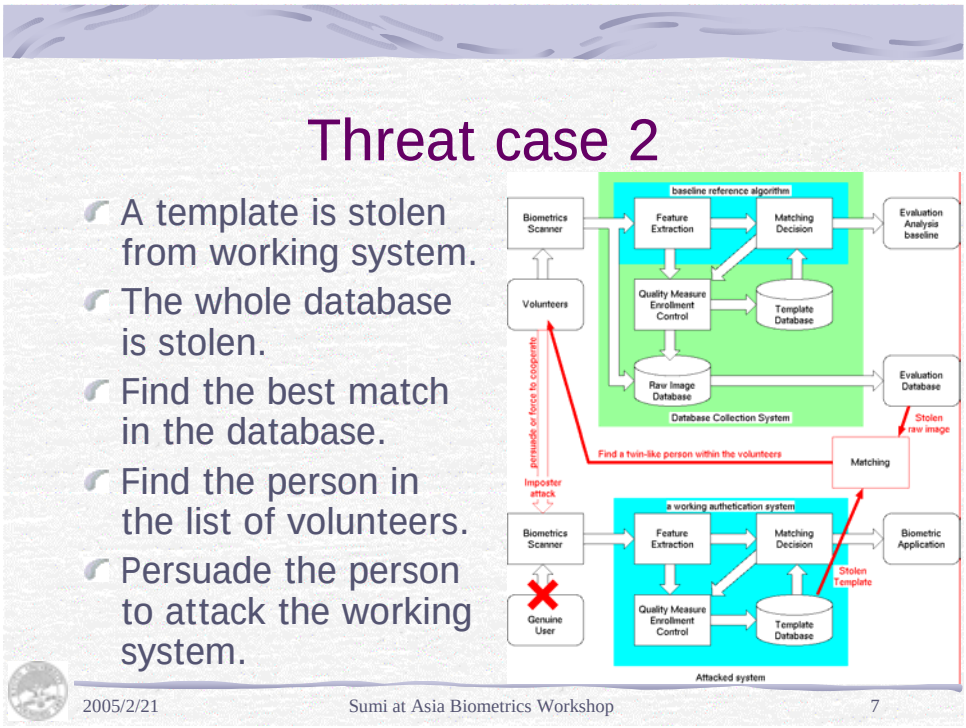


図3 －30　本人データの盗み出しの発生ケース２

（興味本位の検索）被験者のバイオメトリクスデータが了解なしに公開され、興味や娯楽の対象として個人情報が検索されたり、暴露される可能性がある。極端な場合にはストーカ行為などの精神的・肉体的な危害を与えられる可能性もある。（下図 3 －31）

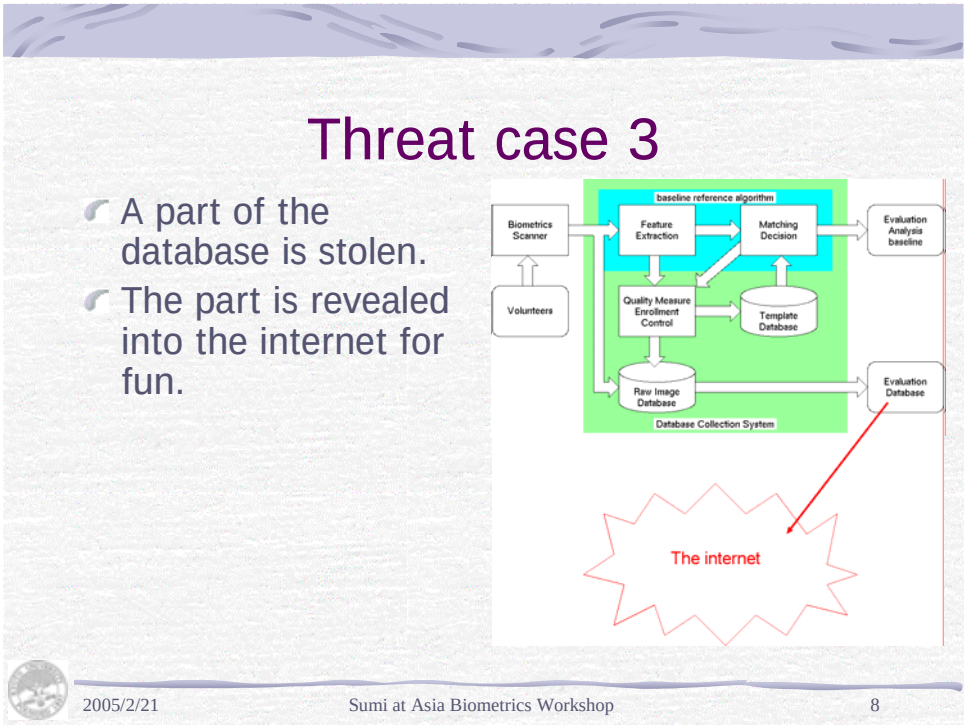


図 3 －31 ： 本人データの盗み出しの発生ケース

このように考えると、評価用データベースといえどもバイオメトリクスデータを不用意に蓄積・流通させることは危険であるという認識に立たねばならない。

一方、実在する生のバイオメトリクスサンプルの収集の困難性や漏洩した場合の危険性を回避するために、バイオメトリクス個人認証の評価に合成されたバイオメトリクスサンプルを用いるという試みも行われている。指紋照合アルゴリズムコンテストである。

Fingerprint Verification Contest (FVC) [Maio-ICBA2004-FVC] では、数種類のセンサーで取得した実在の指紋画像以外に、Bologna 大学で開発された指紋画像生成ソフトウエア SFINGE [Cappelli-ICPR200-Sfinge] が用いられた。指紋照合システムの場合、指紋スキャナ(センサ)が異なれば照合精度の評価結果も大きく違うことが通常であるが、センサー間の違いに比べて実在する指紋と合成された指紋とによる評価結果の違いが特に大きいということはなく、合成された指紋画像も使える可能性が示されている。

図 3 −32 ： 完全に仮想的な評価用指紋画像を生成する Sfinge

指紋の場合には、隆線方向分布には統計的な特徴が認められるが特徴点(マニューシャ)の発生はランダムな要素が大きく、また、我々は多くの人物の指紋画像を見慣れているわけではないため、人工的に生成された指紋画像をみて大きな違和感を感じることはない。

しかし、 顔の場合には、我々自身が顔という画像パターンを日常生活のなかでたいへん注意深くみているため、安易に顔画像を生成しても実在する顔画像とは掛け離れたものになりやすい。また、実際の特徴点分布密度や、隆線の流れ方向の分布などのデータは、あらかじめ与えなければならず、ある被験者の集団を完全にシミュレートするには更なる技術開発を必要としている。

そこで、よりプライバシーの保護が必要となる顔画像を対象に、実画像で構成された会画像データベースから、個人を逆推定することができない仮想的な顔画像データベースを生成する手法について新技術[Sumi-BS-2004]を開発した。

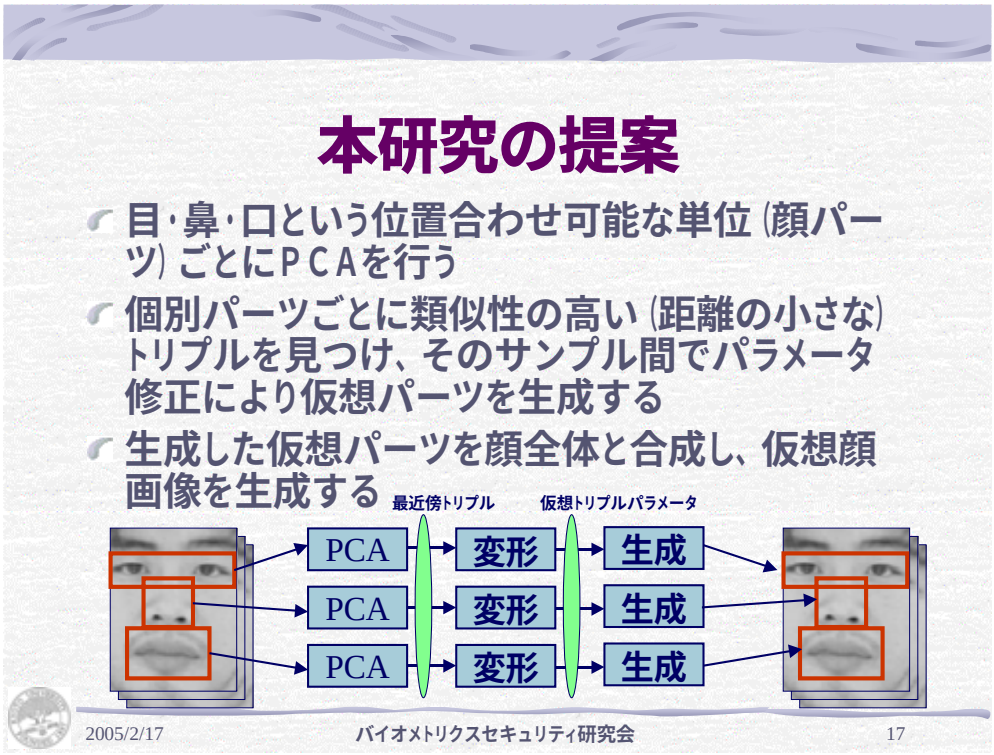


図3 －33 ： 仮想顔画像データベースの生成原理

あらかじめ顔画像中の特徴点を用いて垂直水平の位置と倍率・カメラ光軸回りの回転をアライメントした顔画像を主成分分析して生成される特徴空間において、実在するサンプルの周辺にサンプル点をとり画像空間に逆写像して生成される顔画像を確認した。単純に目の位置で顔画像をアライメントしただけの顔全体の画像から生成された特徴空間の場合には、実在するサンプルの周辺であっても顔パーツ重ねあわせの誤差のためにアーティファクトを発生して実用的な顔画像の生成は不可能であるが、目・鼻・唇のパーツごとに部分領域を生成して同様のことを行うと、それらの主成分部分空間内の実サンプル近傍から逆写像して得られる画像はアーティファクトも少なく実用的であった。

これらの実験結果により、アピアランスベースの部分空間は画像濃度と輪郭の位置の両方に関して両方をパラメータ化した特徴空間において実サンプル近傍点を採用すると実存する顔画像と比べて違和感の少ない顔画像が生成可能であること結論づけられた。

なお、人工的に顔を合成する手法としては、人の顔を平均顔とそれからの変位や、三次元モデル、表情筋肉モデルなどでモデル化し、モデルに基づいて形状やテクスチャを生成する手法など多くの研究事例[Morishima-CVIM139.15-face] がみられるが、本報告では実在する画像データベースを元

にして、その個人認識に対する難易度や特徴を引き継いだ顔画像を生成することに重点をおいている。そのため、この仮想顔画像データベースをアルゴリズム評価に用いても、実画像データベースを用いた場合と極めて近い評価結果が得られることが期待される。具体的な顔画像の生成方法は、技術発表[Sumi-BS-2004][Sumi-ABW-2004][Sumi-FCV-2005] にて行い、参加者のコメントを元に改良を進めている。

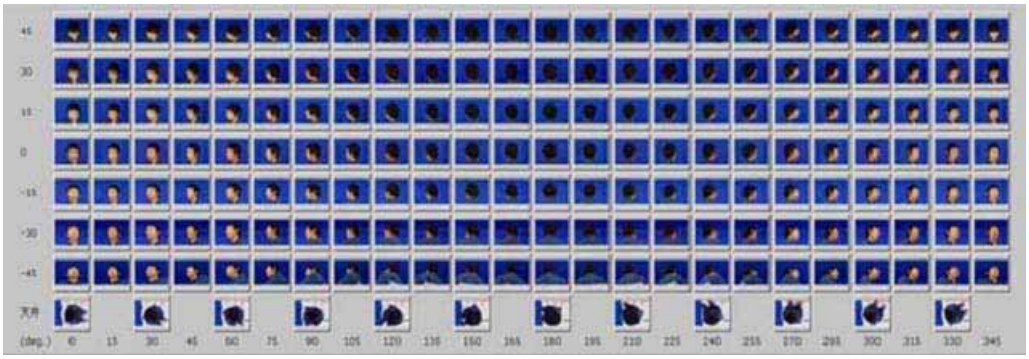


図3 －34　 実験に用いられた実画像の顔画像データベース

ここで紹介する実験結果は、顔画像データベースには、 韓国 POSTECH Intelligent Multimedia Laboratory の Asian Face Image Database PF01 [Postech-PF01] (http://nova.postech.ac.kr/archives/imdb.html) と、HOIP 顔画像データベース [HOIP-face-db] (http://www.hoip.jp/web¥_catalog/top.html) に含まれる正面顔を用いた。PF01 画像データはアジア人の男女１０３名分からなり、１人につき１７のバリエーション(標準、光源違い４、表情違い４、アングル違い４)が含まれており、両目の瞳中心が重なるように位置合わせがなされている。HOIP 画像データベースは ２０－７０才代の男女合計３００名の一般ボランティアの顔画像データベースで、年齢構成と男女比が均一になるように選択されている。HOIP 画像データベースは、精密にはアライメントされていないため、PF01 データベースと同様のアライメントと、同一サイズの切り出しを行った。

本検討では標準の画像から眼鏡をかけていない画像を選び、眉毛・目・鼻・口を含む 112 × 142 の大きさの長方形でトリミングし、以下顔画像として利用する。(図 3 －35) さらに鼻や口など顔の部分画像を用いる場合には、両鼻孔の中心および両唇の中心をそれぞれ画像中心とし画像の切り出しを行った。

図 3 －35　特徴空間における実画像データから仮想画像データの生成原理

図3 －36 ： 仮想的な顔画像データの生成事例（上段：実顔画像、下段：実顔画像から生成された仮想顔画像－実画像の個人とは違う人物に見える）

本検討の実験においては 図3 －36 に示すような仮想画像生成手法を採用した。すなわち実在す

る顔画像のサンプル Pk (1 < k < M) すべてについて、 まず、 互いの距離が Th 以下の 3近傍点 Pk, Pk', Pk'' を選び、それらの平均 C を中心として対称の位置に仮想サンプル点 Qk, Qk', Qk'' を発生させる。もし、 距離が Th 以下に近傍点が存在しない場合には、Pk の位置をランダムに変動させて Qk とした。この方法によって発生させた仮想的な仮想顔サンプル間 (図3 −36 下段) の距離は、上に述べた対称変換の原理によって元になった実サンプル間の距離と同じに保たれており、実サンプルの持つ個性を消しつつ実在するサンプルと同じ距離を持つデータを生成することに成功したと言える。

この方式の改良として、画素の濃度パターンと、 画素の空間方向への移動パターン(あるいは画像の形状変形) との両方でモデル化する手法 (たとえば Active Appearance Model [Cootes-FG00-Viewbased] を導入することで、 さらに自然な顔画像の生成が可能になる。

なお、本検討で未対応の課題として以下のような項目があり、今後順次技術を実装し効果を実証して行く必要がある。

1. 他人間の距離だけでなく本人の変動を考慮したデータ分布を持つ顔画像の生成。 ── 変動を与えた同一人物の顔画像が何枚も得られる場合があり、それに対応して生成する画像でも仮想人物に対して入力と同じ変動を含む仮想画像列を生成することが必要である。個人内変動の統計量を求めておき、平均仮想サンプルを中心に変動を与えるなどの手法がとれる。
2. 眼鏡や髭などコントラストが強く顔を隠すパーツへの対処。── 顔に対してそれを隠蔽するような装着物については、一旦それを分離して、 顔のみの仮想画像を生成した上で書き戻すことが必要である。眼鏡・髭などは外乱として抽出することが可能である。
3. 実際の個人識別アルゴリズムを用いて(元の画像データと同じ)統計的に意味のある精度評価結果が得られるかの検証。特に、アピアランスベースではないアルゴリズムが、本方式で生成される仮想画像データベースに対してどのように振る舞うかについては、今後検討が必要である。

本検討では、実在する人物にから集められた顔画像データベースから、個人識別の精度評価に利用可能で、かつ、実在する顔画像と違和感のない顔画像が生成可能であるか検討を行った。そのために、主成分分析の主成分部分間内での顔画像データの分布を分析し、この、部分空間内で互いに近傍に存在するサンプルを用いて、元のサンプルと同じ相互距離を持ちながら、元画像とは印象の違うサンプルを生成できることを示した。

参考文献:

[Rizvi-FG98-FERET] S. Rizvi, P. Phillips and H. Moon: “The feret verification testing protocol for face recognition algorithms”, AFGR98, pp. 48-53 (1998).

[Maio-ICBA2004-FVC] D. Maio, D. Maltoni, R. Cappelli, J. Wayman and A. K. Jain: “Fvc2004: Third fingerprint verificatin competition”, Proc. International

Conference on Biometric Authentication, pp. 1-7 (2000).
[Cappelli-ICPR200-Sfinge] R. Cappelli, A. Erol, D. Maio and D. Maltoni: “Synthetic fingerprint-image generation”, Proc. International Conference on Pattern Recognition (2000).
[Morishima-CVIM139.15-face] 森島：“顔の分析・合成とその応用”, 情処研報, No. 139-15 in CVIM, pp. 107-114 (2003).
[Sumi-SICE04-face] 鷲見：“顔のバイオメトリクス”, 計測と制御, 43, 7, pp. 554-557 (2004).
[Wiskott-PAMI97-Elastic] L. Wiskott, J. Fellous, N. Kruger and C. von der Malsburg: “Face recognition by elastic bunch graph matching”, PAMI, 19, 7, pp. 775-779 (1997).
[Turk-91-Eigenface] M. Turk and A. P. Pentland: “Eigenfaces for recognition”, CogNeuro, 3, 1, pp. 71-96 (1991).
[Postech-PF01] http://nova.postech.ac.kr/archives/imdb.html.
[HOIP-face-db] http://www.hoip.jp/web catalog/top.html.
[Sung-PAMI98-FaceDetect] K. Sung and T. Poggio: “Example-based learning for viewbased human face detection”, PAMI, 20, 1, pp. 39-51 [Cootes-FG00-Viewbased] T. Cootes, K. Walker and C. Taylor: “View-based active appearance models”, AFGR00, pp. 227-232 (2000).
[Sumi-BS-2004] 鷲見 和彦, 木津 吉博, 松山 隆司, “顔画像の特徴空間内分布の解析と合成 – 仮想顔画像データベースの生成に向けた検討”, 電子情報通信学会, ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会資料, No.3, pp.187-192, 2004
[Sumi-ABW-2005] Sumi K., Matsuyama T., “Privacy Protection of Biometric Evaluation Database - A Preliminary Study on Synthetic Biometric Database”, 2nd Asian Biometric Workshop, no.1, 2004
[Sumi-FCV-2005] Sumi K., Matsuyama T., Privacy Protection of Biometrics Evaluation Database - A Preliminary Study on Synthetic Biometric Database, Korea-Japan Symposium on frontiers in Computer Vision, S74, Jan. 2005

（6）リスク評価のための脆弱性評価

脅威対策の新技術として「テンプレート無効化技術」「データベース保護方式」があるが、生データの照合に比較して、精度低下、処理性能低下、類推可能性の増大、テンプレートデータの逆変換可能性等の脆弱性が想定される。

これらの新技術について、実証実験により脆弱性の評価を行い、実用性を評価する必要があると考えられる。ここでは、新技術の評価方法について今後研究項目として検討するために、実証実験の方法について考察する。

1）テンプレート無効化技術の評価方法

テンプレートの無効化技術を評価するためには、まず、テンプレートからもとのバイオメトリクスデータや別の認証システムを認証するに十分なテンプレートが復元可能かを評価するテンプレート安全性検証と、テンプレートを無効化して再生成した新たなテンプレートが、破棄されたテンプレートと十分異なるかの無効性の検証が必要である。

テンプレート安全性検証技術として、テンプレートから元の顔画像を復元した事例[Adler-2003]があり、このような技術と偽バイオメトリクスサンプル製造技術[Matsumoto-2002]とを組み合わせれば、テンプレートから生のバイオメトリクスデータが得られるかどうかを検証することができる。

なお、現状では生のバイオメトリクスデータを介さずにテンプレートに含まれる秘密鍵を推測する可能性[Uludag-IEEE-2004]も指摘されているが、これらは一般的な暗号解読技術を用いて検証すべきである。

参考事例として Adler らがテンプレートから復元した顔画像の例を示す。

図 3 −37 ：テンプレートさえ手に入れば、下のバイオメトリクスデータ（顔画像）が復元できた事例。本人の顔画像に近い画像（写真右端）を、実験では参照せずに復元した（写真中央と右端）

また、テンプレート無効化を行った場合に、テンプレートを不可視化する変換処理の影響で、認証精度の低下を生じる可能性がある。したがって、同一の評価用データベースを用いて、テンプレート保護を行わない場合と、テンプレートを行った場合とで、認証精度を比較することが必要である。

2）データベース保護方式の評価方法

データベース保護の評価方法は、テンプレート保護の評価方法に準じるが、データベースには元のバイオメトリクスデータがそのまま含まれているので、上記のような復元技術を用いる必要は無く、単純にデータベース内の画像と、登録した実画像との類似度を比較すればよい。

なお、この際、注意すべき点はデータベースの保護操作を行ったために、実画像を用いた場合と異なる評価結果が得られる可能性が発生する点である。その問題を保証する為に、元の実バイオメトリクスデータを保管している機関において、複数のアルゴリズムを用いて精度評価を行い、その精度評価結果（ＲＯＣカーブなど）が二つのデータベース間でほぼ同じであることを検証しなければならない。

「参考文献」

[Matsumoto-2002] Matsumoto T., Matsumoto H., Yamada K., Hoshino S., ``Impact of artificial ¥″gummy¥″ fingers on fingerprint systems'', Optical Sec. and Counterfeit Deterrence Techn. IV. Vol. 4677, SPIE, 2002

[Adler-2003] Adler A., ``Sample images can be independently restored from face recognition template'', Can. Conf. Electrical Computer Eng., pp.1163-1166, 2003

[Uludag-IEEE-2004] Umit Uludag, Sharath Pankanti, Salil Prabhakar , and Anil K. Jain, Biometric Cryptosystems: Issues and Challenges, Proc. IEEE, Vol.92, No.6, pp.948-960. 2004