平成１７年度経済産業省　産業技術研究開発委託事業－１
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

第３部　バイオメトリクスセキュリティ評価基準の開発

平成１８年３月

財団法人ニューメディア開発協会

目　　次

３ バイオメトリクスセキュリティ評価基準の開発

３．１　バイオメトリクスのセキュリティ要件と評価方法の開発

３．１．１　背景と目的

近年、情報システムの安全性に対する要求の高まりから、本人確認手段としてバイオメトリクス技術の適用が進みつつある［1］。バイオメトリクスを情報セキュリティ技術として利用するには、他の情報システムと同様、ＩＳＯ／ＩＥＣ １５４０８［5-１０］（以下ＣＣ：Common Criteria）などによるセキュリティ評価を適用する必要がある［2、3］。

しかし現状では、情報セキュリティの観点に基づいたバイオメトリクスの安全性はまだ十分に検討されていない。バイオメトリクス技術は、本人確認のための識別情報として生体情報を用いているため、生体情報の性質に起因するバイオメトリクス特有の脆弱性を持つ［4］。そのため、一般的なＩＴシステムにおける情報セキュリティの考え方を直接適用することができない。これがバイオメトリクスの安全性評価に関する検討が十分でない一因と考えられる。

バイオメトリクスの安全性評価については、ＣＣの共通評価方法論（ＣＥＭ：Common Evaluation Methodoogy）［９］にバイオメトリクスに関する要件を追加したＢＥＭ（Biometricds Evaluation Methodology）［１３］が知られている。しかしＢＥMが対象としているのは、主にバイオメトリクス装置に含まれる機能間のデータ漏洩や改ざん、推奨環境下で動作させた場合の精度、生体情報の偽造であり、その他のバイオメトリクス特有の脆弱性は触れられておらず、脆弱性分析（ＡＶＡ＿ＶＡＮ）においてバイオメトリクスの専門家の助言を受けるよう提案しているのみである。そのため、現在のセキュリティ評価に関する標準あるいはそれらを補完するドキュメントだけでは、バイオメトリクス装置の評価を実施するのは困難な状況にあるといえる。

そこで本研究では、バイオメトリクス特有の脅威や脆弱性を含めてセキュリティ評価を行うための基盤となる技術あるいは方法論の開発、およびその国際標準化を目的とする。

昨年度の本事業では、一昨年の研究結果に基づき、バイオメトリクス特有の脆弱性の評価方法を検討し、ＳＣ２７案件である１９７９２ " Security evaluation of biometrics "［１４］への貢献を具体的な目標として標準化を進めた。具体的には、特定のターゲットシステムを対象とした場合に、評価者がバイオメトリクス特有の脆弱性を抽出するための要件と参考情報をまとめた。本年度は、これらの作業結果を１９７９２に反映させ、標準文書の一部に展開していくための、標準文書作成および標準化活動を目的とする。

３．１．２　標準化の動向と標準化活動

本節では、バイオメトリクスのセキュリティ標準に関する今年度の動向と、本事業における標準化活動について述べる。主な標準化活動は次表の通りである。

表３－１ 国際標準化活動一覧

#	参加会議・イベント	概要	開催日
1	ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ２７ ウィーン会議	１９７９２ WD３の寄書内容紹介および標準採用に向けた支援作業を目的に参加。１９７９２はWD４へ進行。本会議にてコエディタに就任。	'０５／４
2	１９７９２エディタ会議 （パリ、フランス）	１９７９２ WD４完成に向けたエディタチームによる個別議論および標準文書の作成作業を目的とした会議を実施。	'０５／６
	１９７９２ WD４発行	上記会議に基づき１９７９２の脆弱性分析部分を執筆。正式にＳＣ２７へ提出。	‘０５／７
3	ＳＣ２７／ＷＧ３国内委員会	１９７９２ WD４へのコメント収集を目的にWG３国内委員会にて内容を紹介。委員よりコメントを得た。	'０５／８
4	電子情報通信学会 バイオメトリクス セキュリティ分科会	１９７９２　WD４へのコメント収集を目的に講演	‘０５／１０
5	ＢＳＣ安全性委員会	１９７９２　WD４へのコメント収集を目的に講演	‘０５／１１
6	ＳＣ２７　クアラルンプール会議	１９７９２ WD４に対するコメント処理を目的に出席。すべてのコメントを解決し、ＣＤへの進行が決定。またタイトルを”Security Evaluation of Biometrics”に変更。	‘０５／１０
7	ＳＣ３７　京都会議	ＳＣ３７より１９７９２ WD４に対して150近くのコメントが期限後に提出された。これらのコメントへの対応方針を議論する目的で、エディタとともに本会議に出席。主要なコメントについて議論し、解決を見た。	‘０６／１
8	１９７９２ ＣＤ発行	上記標準化活動において収集したコメントおよびその解決方針に基づき１９７９２ ＣＤの脆弱性分析、用語、参照モデル（Annex A）などを執筆・修正し、正式にＳＣ２７へ投入した。	‘０６／２

●０５年度４月におけるバイオメトリクスのセキュリティ評価標準の状況

１９７９２全体との整合性を確保した脆弱性分析に関する寄書を再度作成し、ＳＣ２７／WG３国

内委員会を通じて国際ＳＣ２７へ正式に寄書を投入［１９］。本寄書はほぼ提出時のまま１９７９２WD３に採用［２０］されている。

１９７９２ WD３はバイオメトリクスのセキュリティ評価に関するフレームワークを定めるものであり、主に以下5点から構成される。

・セキュリティ評価の一般的要件（General requirements of Security Evaluation）
・バイオメトリクスの評価（Evaluation of Biometrics）
　アルゴリズム、装置、システムと環境の３レベルによる評価方針を規定
・エラー率（精度）
　セキュリティの観点からバイオメトリクスの精度評価を実施する上での要件
・脆弱性評価（Vulnerability Assessment）
　バイオメトリクス特有の脆弱性評価に関する要件。
・プライバシ

●ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ２７ ウィーン会議

ＩＳＯ １９７９２は１２月にWD３が公開され、その後カナダ、フランス、米国, オーストラリア、ＳＣ３７からコメントが提出された。今回の会議では、主にこれらのコメントへの対応が審議された。

カナダより、WD3 の内容が主に Informative（参考情報）で構成されているのを理由に、ＩＳ（International Standard）から TR（Technical Report）への変更を求めるコメントがあったが、ＩＳに向けて構成・内容を変更したWD４を作成することでコメントを却下．また，ドキュメントの修正には今後も日本ＮＢ（National Body）貢献が必須であるとの認識から，報告者を acting co-editor に推薦．WG３プレナリ審議で了承された．

●１９７９２エディタ会議（パリ）

先のＳＣ２７ウィーン会議での１９７９２ WD３へのコメントを受け、国際標準に向けて構成・内容を修正し、バイオメトリクス装置のセキュリティ評価要件を明確化することが本会議の主目的である。会議前に作成済みのWD４の素案をベースに、以下の議論およびドキュメント修正を実施した。

・ドキュメント構成：素案からの大きな修正はなく、セキュリティ評価モデル、精度、脆弱性評価、プライバシについての評価要件を記述することで合意
・SC37（バイオメトリクス）標準との整合性：SC37 との整合性を強化するため、バイオメトリクス参照モデルとしてＩＳＯ/ＩＥＣ ＦＣＤ ２４７１３をベースにセキュリティ機能を追加したモデルをAnnex A に記述、用語定義についてはＳＣ３７の参照を大幅に増強する方針とした。
・精度と脆弱性評価：内容に関して詳細にレビューを実施。精度評価に関して、被験者以外の利用者が極端に高い他人受入率を発生させる可能性が指摘され、新たなセキュリティ上の問題点として脆弱性評価に項目が追加された。その他は素案からの大きな修正はなく、エディトリアルな修正にとどまった。
・プライバシ：プライバシ保護を必要とする判断基準について意見がわかれ、結果として評価者が判

断できない場合はプライバシ保護を推奨する記述を盛り込むことで合意。
・本会議での残件をドキュメントに反映し、０５年８月はじめに正式なＷＤ４としてＳＣ２７事務局に提出した。今後ＳＣ２７クアラルンプール会議（１１月）でのＣＤ化を目指す。

●ＩＳＯ １９７９２ ＷＤ４の作成およびＳＣ２７国際委員会への提出
ブラジル会議およびパリ会議での議論を反映し、１９７９２ ＷＤ４の用語、脆弱性分析、参照モデルを作成、エディタによりＳＣ２７へ正式に寄書を投入した［１８］。

●ＳＣ２７／ＷＧ３国内委員会
１９７９２ＷＤ４へのコメント収集を目的にＳＣ２７／ＷＧ３国内小委員会で内容を紹介（付録参照）。得られたコメントおよび議論は以下の通り。

・ＣＣとの関係に関して、１９７９２はＢＥＭで不足している部分である脆弱性評価を補足する標準とも考えられる．ＣＣとの関係については現時点で明確化されていないが，ＣＣフレームワークとは別の標準として考えている．
・１９７９２の利用者として、各国でバイオメトリクスのセキュリティ評価基準を策定する人，あるいはバイオメトリクス製品を作ろうとしている人を想定している。後者の場合は私企業が自社のシステムを評価する際に利用する。Scope に利用者を記述するよう日本コメントに盛り込む．
・１９７９２による評価の実現性に関して、評価を行うレベルによるが、できる範囲で評価すると想定している。例えば，評価のため大規模に生体情報を収集するのは現実的ではないが，アルゴリズムの仕様などを手がかりにすれば，小規模な生体情報データベースでも評価は可能と考えている．具体的な評価のレベルや方法は１９７９２のスコープ外のため記述されていないが、Annex として盛り込めるかエディターチームで検討する．また，本評価に関する認証機関は今のところ存在しない。
・CC フレーム輪ワークに準拠して１９７９２を利用する方策を検討すべき。
・バイオメトリクス用の機能要件および保証要件とあわせて JIL のような位置づけにすべきか。機能要件については 19792 のスコープ外。現時点ではセキュリティ評価の要件をブレークダウンする方向にあり，機能要件を盛り込んで JIL のような位置づけにする考えはエディターチーム内ではあがっていない．
・１９７９２において Vulnerability を一般の意味の Vulnerability とは別の意味で利用しているのであれば、Vulnerability の定義についてきちんと表現するか、もしくは、別の用語を定義すべき。
・脆弱性が脅威にどうつながるかについての記述がない。脆弱性の抽出にあたり想定した脅威があるはず．想定した脅威はある．Annex としてまとめてあるが，完成度が低かったため今回の WD4 からは削除されている．日本コメントに盛り込む．

●ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ２７クアラルンプール会議
同会議に"19792：A Framework of security evaluation for Biometrics"のＷＤ４へのコメント処理およびＣＤへの推進を目的に、コエディタとして出席。
先のエディタ会議にて作成した WD4 に対する各国のコメントを処理し，対応方針（Dispositions of

comments）を作成した。主要な議論は以下の通りである。大幅な修正要求はなく、Committee Draft への進行を提案する決議を得た．ＣＤを'０６/1/３１までに発行し，同時に国際投票にかけられる．

・タイトルの変更：現在の具体的なスコープに沿うため，framework や testing を削除し，"Security Evaluation of Biometrics"に修正．
・Privacy：各国の法などが優先するためＩＳの requirement になじまない（仏）．バイオメトリクスがプライバシに関わるのは明白であり単純に informative とすべきでない（独）．などの意見から IS に組み込むべきか結論に至らず．プライバシ部分を再検討し次回会議で再度議論する．
・CC のバイオメトリクス向け補足情報であるＢＥＭ（Biometric Evaluation Methodology）を１９７９２に盛り込む検討を開始する方針．CCDB で具体的な進展ないため，19792 で扱う方針に変更．
・各国 National Body からのコメントも技術的あるいはエディトリアルなコメントがほとんどであり，ドキュメントとしての構成や大まかな内容については国際的合意が得られたと考える．今後は既に定めた要件を補足する情報を中心に追記を行い，標準文書としての内容充実に努める．具体的には，上記 DoC を基に，CD を作成し１/３１までにＳＣ２７事務局に提出する．主な追記内容は，①脆弱性の評価方針，②脆弱性に関係する脅威の例の二点である．

●ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ３７ 京都会議

前出のＳＣ２７クアラルンプール会議後にＳＣ３７より 150 近いコメントが投入された。コメント期限を過ぎており正式に対応する必要はないものの、有用なコメントが数多く含まれていたため、ＳＣ３７のコメント執筆者と議論して対応方針を決定するため、エディタとともに本会議に出席した。主な議論は各脆弱性項目の定義に関するもので、本議論を元に脆弱性項目の整理を行った。その結果は３．１．３節を参照のこと。また、脆弱性の評価に関して具体的な要件が不明とのコメントがあり、開発者および評価者のとるべきアクションの形で記述する方針とした。

●ＩＳＯ １９７９２ ＣＤの作成およびＳＣ２７国際委員会への提出

上記クアラルンプール会議および京都会議での議論を反映し、１９７９２ＣＤを作成し、エディタより国際ＳＣ２７へ正式に寄書を投入［１４］。今後、約３ヶ月間の投票期間を経て、'０６／５のＳＣ２７ マドリッド会議にて内容が審査される予定である。

３．１．３　脆弱性評価に関する要件

ＷＤ３における脆弱性分析は、バイオメトリクスセキュリティ評価の基本モデルである３レベル評価（アルゴリズム、装置、運用システム）の各レベルについて、評価すべき脆弱性を定義したものである。

ＷＤ４およびＣＤへの移行にあたって行われた主要な修正は以下の通り。

①脆弱性項目の見直し

②脅威の記述追加

③脆弱性項目と評価レベルの関係整理

以下それぞれの修正点について具体的に説明する。詳細な内容については１９７９２ＣＤ［１４］を参照のこと。

①脆弱性項目の見直し

主にＳＣ３７のバイオメトリクスの専門家からのコメントに従い、脆弱性項目を再度整理した。具体的な変更点とその理由を以下に示す。

・生体情報の偽造（Imitation of biometric characteristics）

人工物による偽造と、本物の生体情報を体から切り離した偽造とを混同していたため、それらの対策を分けると同時に脆弱性項目も明確に分離した。すなわち、「偽造」とは何らかの人工物により生体情報と同じような観測データを与えるものを指す。この場合の「偽造の脆弱性の程度」とは、人工物により偽造物を生成する難易度を意味する。またこの脆弱性への対策はなんらかの偽造検知技術（Imitation Prevention）によってなされる。一方、人体から生体情報を切り離した場合、偽造検知とは異なる技術（例えば生体検知技術（livenss checking））が必要になる。そこで不十分な生体検知機能が原因で人体から切り離された生体情報をバイオメトリクス装置が受け入れてしまう脆弱性を「偽造」とは別途「不十分な生体検知（Deficient liveness check）」として定義した。この脆弱性の程度は、人体から切り離された生体情報がバイオメトリクス装置に受け入れられる時間を考慮して決定される。

・ものまね（Mimicry of biometric characteristics）

対象とするバイオメトリクス技術の範囲を行動的特徴に限定

・不十分な生体検知（Deficient liveness check）

上記「生体情報の偽造」で述べたとおり、偽造とは別の脆弱性として定義した。

・被験者の偏り（Bias of the target population ）

脆弱性の項目から削除した。本脆弱性は、被験者が一般的な利用者を代表しておらず生じる偏りにより、精度評価で得られた精度を運用時に再現できず、安全性が低下することを意味する。例えば、

解像度の十分でない指紋センサを用いていると仮定して、隆線幅の広い被験者（例えば男性）のみで精度評価を行った場合、隆線幅の狭い利用者（例えば女性）による FAR が、評価結果の FAR から大きく上昇する現象などである。この現象はバイオメトリクス装置の仕様に起因して生じるが、適切な精度評価を実施することによって回避することも可能である。したがって、この問題はセキュリティを考慮した精度評価の要件として記述すべきである。１９７９２ ＣＤでは、精度評価の項にこの問題を記載した。

・経時変化（Aging of biometric characteristics）
　生体情報を登録した後の経過時間により精度が変化することが一般に知られているが、この現象は主にＦＲＲについて生じるものであり、ＦＡＲにおいて問題になる可能性は低い。そのため本脆弱性は削除された。

・センサ（Capturing）
　本脆弱性はセンサの汚れなどにより精度（ＦＡＲ）が影響を受ける可能性を示していたが、環境（Unexpected Environment）との明確な区別が困難であることから、本脆弱性は環境に関する脆弱性に統合した。

・整合性（Consistency of biometric component）
　本脆弱性はバイオメトリクス装置を構成するサブコンポーネントの整合性が保たれないため（例えば一部のサブコンポーネントを更新した場合など）にＦＡＲが著しく大きくなる脆弱性を示していたが、ＦＡＲを増大させる可能性は低いとの指摘を受け、削除した。

②脅威の記述追加
　読者の理解を助けるため、脆弱性の選定にあたり想定している脅威を記述すべきとのコメントを受け、本ドキュメントで想定している脅威の分類および各脆弱性項目において想定した脅威を記述した。以下に具体的に示す。詳細は１９７９２ ＣＤを参照のこと。

【脅威の分類】
・意図的ななりすまし
　攻撃者は潜在的な脆弱性を利用し、認証あるいは識別の際に正規の利用者になりすまそうとする。
・偶発的ななりすまし
　潜在的な脆弱性が原因で、通常の FAR よりもはるかに高い率で利用者が他の正規の利用者としてシステムに受け入れられる。
・バックドアの生成
　登録プロセスにおいて一人以上の攻撃者を受け入れうるアカウントを生成する。

以下に脅威の記述例を示す。下線は脅威について言及している箇所である。

【例：６．３．１ 生体情報の偽造（Imitation of biometric information）】

生体情報は IC カードや鍵のように偽造を防止するように設計されているわけではない。グミによる指紋や録音した音声など、誰でも簡単に偽造しうる生体情報が存在する。これは利用者のなりすましやバックドアの生成につながる潜在的な脆弱性である。

この潜在的な脆弱性が簡単につけこまれない（exploit）ことを確認するために、開発者は製品の偽造防止に関する情報を提供しなければならない。この情報は以下を含むべきである。偽造の難易度、キャプチャサブコンポーネントおよび偽造防止サブコンポーネントの仕様、ターゲットシステムが仮定する環境および運用条件。さらに開発者はターゲットシステムにおける偽造困難性を主張しなければならない。開発者は、偽造の作成に関するテスト結果を提出してもよい。加えて、偽造防止の効果に関するあらゆる制限事項が明示されなければならない。評価者は開発者の主張を検証する目的で偽造防止を評価しなければならない。さらに一般的に知られているバイオメトリクス技術に関係した偽造の方法の可能性を評価するために、評価者は他の利用可能な偽造技術を利用しなければならない。これらの要件はシステムレベル評価に適用される。

もし上記の評価の結果、偽造防止の性能に関する不足が明らかになった場合、評価者はさらに以下の脅威についても評価しなければならない。

この脆弱性につけこむ脅威のひとつは特定の利用者の生体情報に良く似た生体情報を与える人工物を使った意図的ななりすましである。この攻撃にはオリジナルのバイオメトリクスサンプルが必要になるため、評価者はこの脅威に対する抵抗性を評価するためにオリジナルの生体情報を入手する場合の困難性も考慮すべきである。この脅威の評価を可能にするために、開発者はオリジナル生体情報を入手するための困難性（６．３．４、６．３．１１に記述）に関する情報を提供しなければならない。開発者はまた、ターゲットシステムがこの脅威に対して耐性があることを主張しなければならない。

もうひとつの脅威は、偽造物を用いた登録時のバックドアの生成である。偽造物が登録され照合される場合、偽造物が誰でもシステムにアクセスできるトークンとして利用される可能性がある。この場合、偽造物は正規の利用者の生体情報を与える必要はないため、攻撃者はオリジナル生体情報を入手する必要はない。一方、この脅威を評価するためには、開発者は登録時の運用要件に関する情報を提供し、ターゲット製品がこの脅威に対して耐性を有していることを主張しなければならない。例えば、管理者によりモニターされた登録プロセスは効果的な対策になりうる。評価者は開発者の主張の妥当性を検証しなければならない。これらの要件はアプリケーションレベル評価に適用される。

③脆弱性項目と評価レベルの関係整理

各脆弱性項目は全ての評価レベルで評価しなければならないわけではない。１９７９２CD１では、脆弱性項目と評価レベルの関係について以下のように記述を追加している。

【６．３ Vulnerability Assessment より抜粋】

脆弱性評価に関する要件は下表に示すように評価レベルに依存している。表は各潜在的な脆弱性への要件を評価レベルごとにまとめたものである。“N/A” はその評価レベルにおける脆弱性評価を行う必要がないことを意味する。“基本的（Basic）”評価は、その評価レベルにおいて、単一の潜在的脆弱性の度合いを明らかにする評価を意味する。“拡張（Extended）”評価は、その評価レベルにおいて、

ターゲット（アルゴリズム、装置、システム）がその潜在的脆弱性に関係する脅威に対して耐性を有することを確認することを意味する。また、評価レベルは階層構造を持っており、常に上位の評価レベルは下位の評価レベルを含まなければならない。すなわち、拡張評価（Extended）を実施するということは、同時に基本評価（Basic）も実行することを意味する。しかし、基本評価において単一の脆弱性が簡単に悪用（exploit）されないことが確認できている場合、拡張評価を行う必要はない。したがって、システムレベル評価あるいはアプリケーションレベル評価においては、まずコンポーネントレベル評価から着手することが効果的である。

Subclause	Potential Vulnerability	Component	System	Application
4.3.1	Imitation	N/A	Basic	Extended
4.3.2	Mimicry	Basic	Extended	Extended
4.3.3	Deficient liveness check	N/A	Basic	Extended
6.3.4	Impossibility of concealing biometric characteristics	N/A	Basic	Extended
6.3.5	Similarity	Basic	Extended	Extended
6.3.6	Special biometric characteristics	Basic	Extended	Extended
6.3.7	Synthesised biometric samples	Basic	Extended	Extended
6.3.8	Unexpected Environment	N/A	Basic	Extended
6.3.9	Configuration	N/A	Basic	Extended
6.3.10	Enrolment process	N/A	N/A	Basic
6.3.11	Leakage and alteration of biometric data	N/A	Basic	Extended

Table 2: Vulnerability assessment based on the three levels of evaluation

３．１．４　セキュリティ評価におけるバイオメトリクスシステムの参照モデル

セキュリティ評価におけるバイオメトリクスシステムの参照モデルは、ＩＳＯ／ＩＥＣ ＦＣＤ ２４７１３－１ Biometric Profiles for Interoperability and Data Interchange – Part 1: Biometric Reference Architecture［１７］を基にして、セキュリティ評価に必要なサブシステムを追加したものである（下図)。具体的には、１９７９２の Annex A に記載されている。

ＣＤの作成にあたって大きな変更はなく、用語をＳＣ３７ ＳＤ２．４［１６］に沿って修正し、識別（Identification）システムに関するプロセスを追加したのみである。

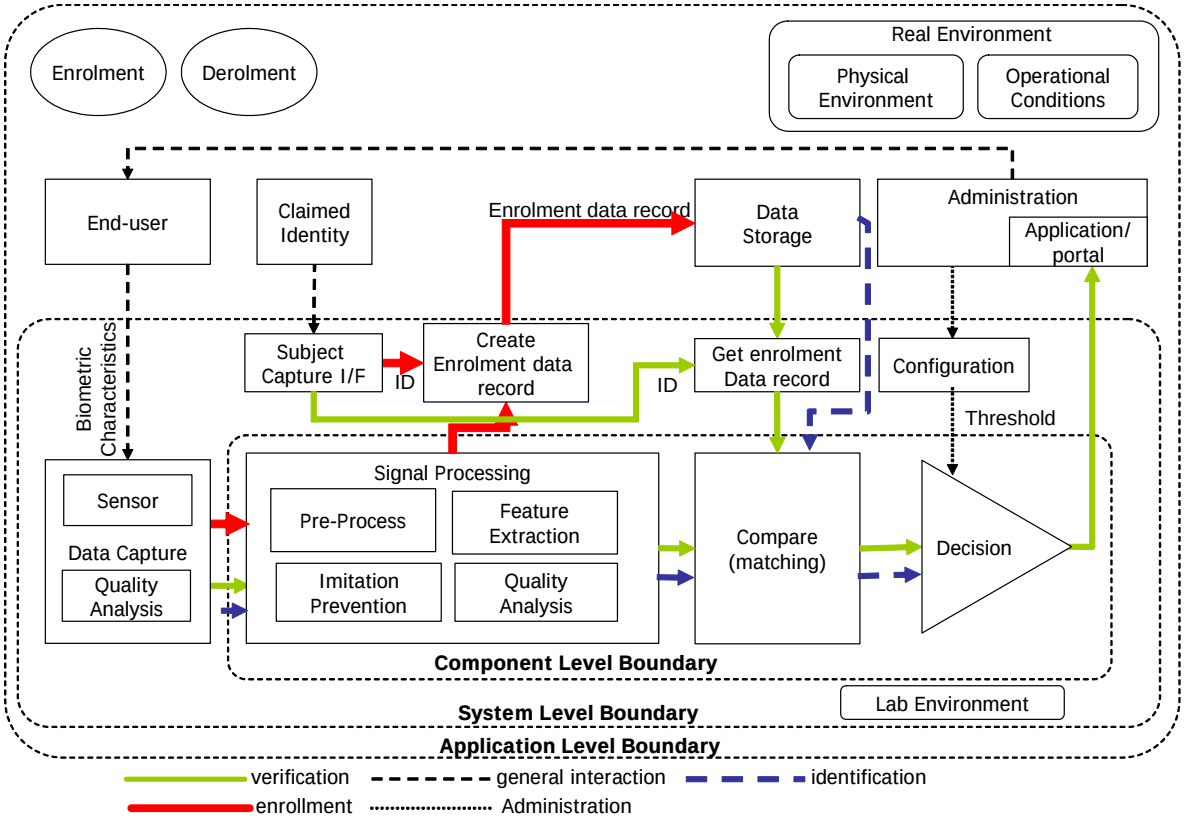

Enrolment
Derolment
Real Environment
Physical Environment
Operational Conditions
End-user
Claimed Identity
Enrolment data record
Data Storage
Administration
Application/ portal
Biometric Characteristics
Subject Capture I/F
ID
Create Enrolment data record
ID
Get enrolment Data record
Configuration
Threshold
Sensor
Data Capture
Quality Analysis
Signal Processing
Pre-Process
Feature Extraction
Imitation Prevention
Quality Analysis
Compare (matching)
Decision
Component Level Boundary
System Level Boundary
Lab Environment
Application Level Boundary
verification
general interaction
identification
enrollment
Administration

図３－１　参照モデル

３．１．５　脆弱性評価方法

より具体的な脆弱性評価を記述する目的で、１９７９２CD１では脆弱性の評価方法に関する記述を追加した。ただし、具体的な評価方法は１９７９２のスコープではないため、開発者および評価者が実行すべき要件を規定するに留めた。

１９７９２CD１では、脆弱性の評価において、開発者（Vendor）と評価者（Evaluator）の役割を定めている。開発者は評価者が評価を実施するために必要な情報を提供し、１９７９２CD１に列挙されている脆弱性および関連する脅威に対して十分な耐性があることを主張しなければならない。評価者は開発者から提供された情報にもとづき、その主張の妥当性を確認する。必要であれば評価者は追加の独立テストを行うこともある。

【開発者】：脆弱性評価を受けるアルゴリズム、装置、またはシステムの開発者あるいは専門家
【評価者】：開発者から提供される情報に基づき、開発者の主張の妥当性を検証する

これは、脆弱性の評価に開発者の協力が不可欠であると考えられるためである。１９７９２で扱う脆弱性はバイオメトリクスに特有であり、そのためターゲットとなるバイオメトリクス認証装置のアルゴリズムや実装に深く関係する。評価者が開発者と同等の技術的スキルを持つとの仮定は現実的でないため、開発者が必要な情報を提供し、評価者がその妥当性を検証することで、脆弱性の評価を実施する方針を採っている。

脆弱性評価のプロセスにおける開発者と評価者の基本的な役割および実施項目は以下の通りである。

ア）開発者は脆弱性に関する情報を評価者に提供する。
　　提供すべき情報は個々の脆弱性に関して定義されている。
イ）開発者は脆弱性が簡単に利用（exploit）されないことを主張する。
ウ）評価者は開発者の提供する情報に基づき、イ）の主張の妥当性を検証する。
　　必要であれば評価者は独自のテストを実施することもできる。
エ）上記検証の結果、脆弱性が悪用される可能性があると判断された場合、以下の評価を実施する。
オ）開発者は脆弱性を組み合わせた脅威に対するターゲットの耐性を示す情報を提供する。
　　脆弱性を組み合わせた脅威は個々の脆弱性に関して定義されている。
カ）開発者は上記脅威に対してターゲットが十分な耐性を有していることを主張する。
キ）評価者は開発者の提供する情報に基づき、カ）の主張の妥当性を検証する。
　　必要であれば評価者は独自のテストを実施することもできる。

以下に具体的な例を示す。下線が開発者と評価者の基本的な役割および実施項目を示す。

【例：６．３．１ 生体情報の偽造（Imitation of biometric information）】

生体情報は IC カードや鍵のように偽造を防止するように設計されているわけではない。グミによる指紋や録音した音声など、誰でも簡単に偽造しうる生体情報が存在する。これは利用者のなりすまし

やバックドアの生成につながる潜在的な脆弱性である。

この潜在的な脆弱性が簡単につけこまれない（exploit）ことを確認するために、開発者は製品の偽造防止に関する情報を提供しなければならない。この情報は以下を含むべきである。偽造の難易度、キャプチャサブコンポーネントおよび偽造防止サブコンポーネントの仕様、ターゲットシステムが仮定する環境および運用条件。さらに開発者はターゲットシステムにおける偽造困難性を主張しなければならない。開発者は、偽造の作成に関するテスト結果を提出してもよい。加えて、偽造防止の効果に関するあらゆる制限事項が明示されなければならない。評価者は開発者の主張を検証する目的で偽造防止を評価しなければならない。さらに一般的に知られているバイオメトリクス技術に関係した偽造の方法の可能性を評価するために、評価者は他の利用可能な偽造技術を利用しなければならない。これらの要件はシステムレベル評価に適用される。

もし上記の評価の結果、偽造防止の性能に関する不足が明らかになった場合、評価者はさらに以下の脅威についても評価しなければならない。

この脆弱性につけこむ脅威のひとつは特定の利用者の生体情報に良く似た生体情報を与える人工物を使った意図的ななりすましである。この攻撃にはオリジナルのバイオメトリクスサンプルが必要になるため、評価者はこの脅威に対する抵抗性を評価するためにオリジナルの生体情報を入手する場合の困難性も考慮すべきである。この脅威の評価を可能にするために、開発者はオリジナル生体情報を入手するための困難性（６．３．４、６．３．１１に記述）に関する情報を提供しなければならない。開発者はまた、ターゲットシステムがこの脅威に対して耐性があることを主張しなければならない。

もうひとつの脅威は、偽造物を用いた登録時のバックドアの生成である。偽造物が登録され照合される場合、偽造物が誰でもシステムにアクセスできるトークンとして利用される可能性がある。この場合、偽造物は正規の利用者の生体情報を与える必要はないため、攻撃者はオリジナル生体情報を入手する必要はない。一方、この脅威を評価するためには、開発者は登録時の運用要件に関する情報を提供し、ターゲット製品がこの脅威に対して耐性を有していることを主張しなければならない。例えば、管理者によりモニターされた登録プロセスは効果的な対策になりうる。評価者は開発者の主張の妥当性を検証しなければならない。これらの要件はアプリケーションレベル評価に適用される。

３．１．６　結論

(1)　国際標準化の成果と今後の課題

国際標準化に関し、今年度は、本事業成果を展開したＩＳＯ　１９７９２　"Security Evaluatoin of Biometrics"の標準化を推進することを目的に、ドキュメント作成、国内標準化活動、および国際標準化活動に参加した。主な標準化活動は以下の通りである。

表３－３　標準化活動一覧

#	参加会議・イベント	概要	開催日
1	ＩＳＯ／ＩＥＣ　ＪＴＣ１　ＳＣ２７　ウィーン会議	１９７９２ WD３の寄書内容紹介および標準採用に向けた支援作業を目的に参加。１９７９２はWD４へ進行。本会議にてコエディタに就任。	'０５／４
2	１９７９２エディタ会議（パリ、フランス）	１９７９２ WD４完成に向けたエディタチームによる個別議論および標準文書の作成作業を目的とした会議を実施。	'０５／６
3	ＳＣ２７／ＷＧ３　国内委員会	１９７９２ WD４へのコメント収集を目的にWG３国内委員会にて内容を紹介。委員よりコメントを得た。	'０５／８
4	電子情報通信学会　バイオメトリクスセキュリティ分科会	１９７９２　WD４へのコメント収集を目的に講演	‘０５／１０
5	ＢＳＣ安全性委員会	１９７９２　WD４へのコメント収集を目的に講演	‘０５／１１
6	ＳＣ２７　クアラルンプール会議	１９７９２ WD４に対するコメント処理を目的に出席。すべてのコメントを解決し、ＣＤへの進行が決定。またタイトルを”Security Evaluation of Biometrics”に変更。	‘０５／１０
7	ＳＣ３７　京都会議	ＳＣ３７より１９７９２ WD４に対して150近くのコメントが期限後に提出された。これらのコメントへの対応方針を議論する目的で、エディタとともに本会議に出席。主要なコメントについて議論し、解決を見た。	‘０６／１

以上の標準化活動を通じ、本事業で作成したバイオメトリクス特有の脆弱性抽出に関する方法論および参考情報を、ＩＳＯ　ＣＤ１　１９７９２（Committee Draft）として結実させることができた。

（2）　技術開発の成果と今後の課題

技術開発に関し、今年度は１９７９２の標準化推進を目標として、これまでの成果を標準文書に展

開するための技術開発を行った。具体的には、評価対象のターゲットシステムごとに、脆弱性を評価するための開発者および評価者の要件をまとめた。これらの要件には、各脆弱性を評価する場合に詳細に調査が必要となる情報を含んでいる。１９７９２のスコープは具体的な評価方法の規格化を目的としていないため、開発者および評価者が検討しなければならない情報を既定することで、これまでに本事業で検討した脆弱性評価方法に関する知見を盛り込んだ。

（3）　当初の目標に照らした達成状況とその要因

今年度は、本事業の最終年度（3年目）であり、バイオメトリクスのセキュリティ評価に関する標準策定を進めることが目標である。この目標に対し、今年度は１９７９２ ＷＤ４の作成、国内でのコメント収集、国際標準化会議での調整活動などを実施し、ＣＤへ進むことができた。最終的には来年度の各国からのＣＤ投票によりＣＤ化の承認が決まる。

本事業を開始した当初は技術開発を進めながら標準化提案先を模索していたが、最終年にあたってその成果をＣＤに結実させ、当初の目的を十分に達成することができたと考えている。

３．１．７　参考文献

［1］瀬戸編著「ユビキタス時代のバイオメトリクスセキュリティ」日本工業出版、２００３

［2］瀬戸”サイバーセキュリティにおける生体認証技術”、共立出版（２００２／５）

［3］磯部“バイオメトリクス技術最前線ーバイオメトリクス技術とセキュリティ標準”月刊バーコード２００２年６月号、日本工業出版（２００２／６）

［4］三村ほか「生体認証における脅威および脆弱性に関する分析」、電子情報通信学会 バイオメトリクスセキュリティ研究会、２００３

［5］ＩＳＯ／ＩＥＣ　１５４０８　: Information technology - Security techniques - Evaluation criteria for ＩＴ security、１９９９

［6］JIS X ５０７０、セキュリティ技術-情報技術セキュリティの評価基準、２０００

［7］永井ほか”情報システムに対するセキュリティ国際評価基準の動向と日立製作所の対応”、日立評論 Vol.８１ No.６(１９９９／６)

［8］永井ほか” セキュリティ対策目標の最適決定技法の提案”、 情報処理学会論文誌、Vol.４１、No.８、２２６４-２２７１（２０００／８）

［9］"Common Evaluation Methodology for Information Technology Security Evaluation (CEM)、" CEM-９７／０１７、CEM-９９／０４５

［10］IPA（情報処理振興事業協会）セキュリティセンター翻訳 「情報技術セキュリティのための共通評価方法論」

［11］"Biometric Device Protection Profile (Draft Issue ０.８２)、" Communications-Electronics Security Group、 Biometric Working Group、２００１

［12］"Biometric Verification Mode Protection Profile for Medium Robustness Environments (version １.０)、" National Security Agency、２００３

［13］"Biometrics Evaluation Methodology、" Biometric Evaluation Methodology Working Group、 ２００２

［14］ＩＳＯ／ＩＥＣ ＪＴＣ １／ＳＣ ２７ Ｎ４８９６、 ISO/IEC 1st CD 19792 Information technology — Security techniques — Security evaluation of biometrics

［15］ＩＳＯ／ＩＥＣ ＪＴＣ １／ＳＣ ２７ Ｎ３９８８、 Japanese National Body comments received on document ＳＣ２７ Ｎ３８０６ - ＩＳＯ／ＩＥＣ １st WD １９７９２ - A framework for security evaluation and testing of biometric technology

［16］ＩＳＯ／ＩＥＣ ＪＴＣ １／ＳＣ ３７ Ｎ１２４８、Text of ISO/IEC JTC 1/SC 37 Standing Document 2 (SD 2), Harmonized Biometric Vocabulary

［17］ＩＳＯ／ＩＥＣ ＪＴＣ １／ＳＣ ３７ Ｎ１２２６、 Text of FCD 24713-1, Biometric Profiles for Interoperability and Data Interchange – Part 1: Biometric Reference Architecture

［18］ＩＳＯ／ＩＥＣ ＪＴＣ １／ＳＣ ２７ Ｎ４４９９、 Text for ＩＳＯ／ＩＥＣ 4th WD １９７９２ — Information technology — Security techniques — A framework for security evaluation and testing of biometric technology

［19］ATTACHMENT ３ TO ＳＣ ２７ Ｎ４１４４、Japanese comments on ＩＳＯ／ＩＥＣ 2nd WD

１９７９２
[20] ＩＳＯ／ＩＥＣ ＪＴＣ １／ＳＣ ２７ Ｎ４２４７、 Text for ＩＳＯ／ＩＥＣ 3rd WD １９７９２ — Information technology — Security techniques — A framework for security evaluation and testing of biometric technology

３．２　バイオメトリクスの脅威・脆弱性公開におけるガイドライン策定

＜担当：早稲田大学・小松＞

（１）はじめに

技術に完全ということは無く、常に脆弱性が伴う。この脆弱性を発見した場合、どのように事実を公開し、問題点に対応すべきか。こうした検討は、システムを健全に構築し、かつ運用するうえで不可欠であることは言うまでもない。

バイオメトリックシステムにおいても、生体情報、バイオメトリック装置とともにそれらの運用・管理の観点から脅威と脆弱性の存在を明確にしてそれらを公開することは、迅速かつ的確な対策を講ずるうえで重要である。例えば情報通信倫理綱領[1]（社会的責任）でも指摘されているとおり、新技術の研究開発と運用に当たっては、技術がどのような社会的影響を与えるかを明確にし、影響に関する情報を広く周知する努力が要請されている[2]。ここでは、専門家として技術とその運用に関する正しい理解が必要とされており、一般利用者に対しても分かり易く説明する義務が求められる。

バイオメトリクスの脅威･脆弱性公開におけるガイドラインは､個人また組織において認証システム、装置の脅威と脆弱性を発見した際の行動規範の拠り所となるものであり、開発・運用者、利用者の立場を十分考慮して取りまとめる必要がある。

本節では､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（以下、BS 研究会）（委員長：半谷精一郎教授（東京理科大））において 2005 年 9 月に開催されたパネル討論の概要をまとめ、ガイドライン策定の方針を考察する。

（注１）

（２）ガイドライン策定方針

脆弱性の発見から製品開発者による対策が円滑に進めば脆弱性に基づく脅威は発生しないが､実際には以下の問題が存在する[3]。

１）発見された情報に関する情報の暴露、流出

・発見者が脆弱性に関する情報を掲示板等に暴露
・発見者が脆弱性に関する情報を放置
・製品開発者などが脆弱性に関する情報を放置
・一部の製品開発者だけが対策を公開

２）利用者の対応が攻撃の開始に間に合わない

このように、発見者、製品開発者、利用者が相互に関連を持つことから、全体を考慮した情報の取り扱いと対処が必要となることが分かる。

文献[4]（平成 16 年度経済産業省委託事業成果報告抜粋）によれば、公的な機関で、詳細ガイドライン作成および管理体制を構築することが急務であり、バイオメトリック製品の脆弱性発見の場合の対応フローとして図１が提案されている。

①製品開発者は、事前に十分な脆弱性脅威対策を行った上で製品を出荷する。脆弱性情報が存在する場合、受付機関に情報を事前に提供する。

②製品開発関係者以外の脆弱性の発見者は、一般の場に情報を公開する前に受付機関および調整機関との調整を行う。脆弱性の詳細の情報の公開は好ましくなく、公開は脆弱性の存在のみに留める。
③一般利用者への情報公開は、調整機関でその効果を判断した上で行う。
④運用者には、受付機関に脆弱性情報が入った時、および調整機関での検討を行った時、迅速な情報の提供を行う。
⑤対策技術に関しては、一般利用者への公開は不要であり、調整機関、製品開発者、運用者の間で共有する。

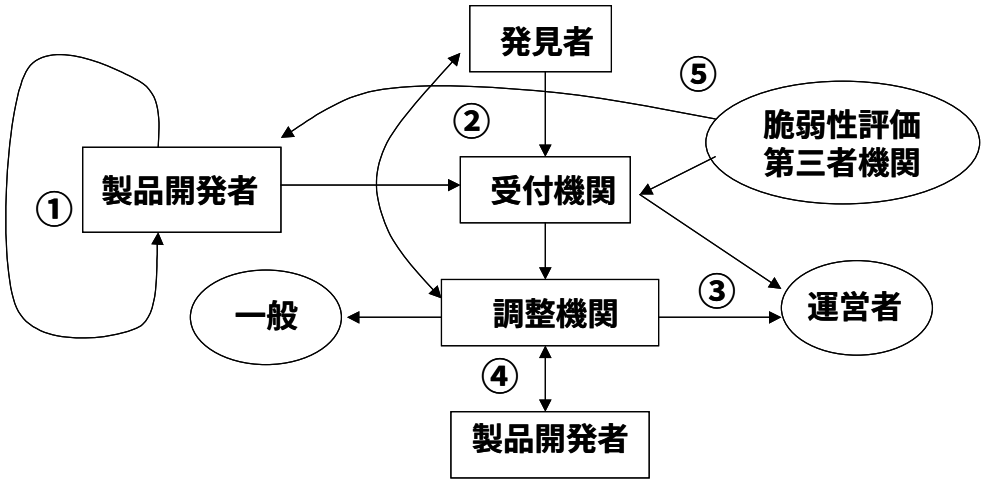


図１ バイオメトリック製品の脆弱性発見の場合の対応フロー案

（３）バイオメトリック認証の脆弱性

図１に示すバイオメトリック製品の脆弱性発見の場合の対応フロー案を共通認識として､バイオメトリック認証の脆弱性に関するパネル討論を電子情報通信学会 BS 研究会で行った｡本節ではその概要をまとめる。

１）バイオメトリクス個人認証の脆弱性保護技術[5]

a) 脆弱性に関する背景－バイオメトリクス個人認証への期待と現実－

・既存の個人認証の弱点克服

弱点= 偽造・盗難・協力・強制

・方法は違うだけで同じ弱点を攻撃可能

・偽造可能性

偽造した生体情報の提示

・盗難可能性

本人が認知しない生体情報と登録情報の漏洩や改竄

・協力可能性

本人が意図的・強制的に協力

b) 攻撃耐性技術

・偽造
生体検知機能による防御
・盗難
暗号化
登録の無効化
遺留・露出の抑制
・協力・強制
定形外行動の自動検出と単独認証の抑制

c) 生体検知
・静的特長
・形状・模様・（スペクトル）反射率・導電率・誘電率・水分含有率・特定化学物質・硬度・温度
センシング手法が確立されれば、情報処理としては単純
原理と入手法がわかれば偽造可能
・動的特徴
・随意運動・不随意運動・刺激に対する反射
静的特徴より模倣するためにコストがかかるのでより安全動的事象の処理コストが大きい
・どこまで実装されるか
・守るべき価値・攻撃可能性・対策コストのトレードオフ
現状で偽造による被害が深刻でなく導入が進んでいない

d) 登録無効化
・公開鍵でテンプレートの真正性を保証
・奪われたテンプレートの真正性を否定できる
・無効化可能なバイオメトリクステンプレート
・方式提案が行われている段階だが、将来必要な技術
Cancelable Biometrics / Key Hiding / Key Generation

e) Key Generation の研究例
・Fuzzy commitment (Jules, 1999)
完全に一致しないが、ほどほどに近い秘密鍵が受け入れられる暗号化理論
・Fuzzy vault (Jules, 2002)
秘密鍵のビット順序の入れ替わりを許容
・Fuzzy fingerprint vault (Clancy, 2003)
Fuzzy vault が指紋に適用可能なことを提案
・Fuzzy fingerprint vault (Yang, 2004)
課題となる位置合わせを三点間の不変特徴で解決

f) 提言
・検知は効果的なものを追求
・詐称の難しさ×検知簡単さ
・テンプレートの保護はすぐにでも必要

・当面はテンプレート暗号化で対処
・無効化可能な暗号化テンプレートの開発が急務
・詐称の可能性は決してなくならない
・バイオメトリクスへのIDS（定型的認証パターンを学習し、定形外行動を検出）
・不審行動の人による監視の必要性

２）金融業務とバイオメトリクス[6]

a) 現在のキャッシュカードと ATM による預金引出しの脆弱性
・偽造の容易な磁気ストライプカード
⇒ IC カード化による対応が進められつつある。
・4 桁の暗証番号の限界
⇒ 利用者による不適切な設定・運用を排除できないため、推定されたり、銀行システムの外部で漏洩してしまうリスクがある。

b) 金融業界がバイオメトリクスに求めるもの
・偽造対策としてキャッシュカードを IC カード化したとしても、盗用までも防止できない。盗難カードによる被害を防ぐためにも、暗証番号よりも高度な本人確認手段が必要。
⇒ IC カードに加えてバイオメトリクスを導入する動き
・金融機関相互の CD オンライン提携と、バイオメトリクス認証技術間の相互運用性、互換性の問題
・預金取引に対する信頼を取り戻す手段として、どこまで評価できるか （膨大な導入コスト、代替手段との比較）
・「バイオメトリクスは究極のセキュリティ対策」 というイメージが先行している一方、実際のシステムに実装した場合の、運用面を含めたセキュリティを正確に評価することが困難であるため、方針を決めかねている利用者が多い。
⇒ 安全性評価に対する正確な理解が必要

c) 今後のバイオメトリクス研究の課題
・バイオメトリクスによる安全性を、正確に評価するための枠組み作りと、ユーザの正しい理解。
・特に、バイオメトリクスを利用したシステムに固有の「身体的特徴の偽造による攻撃」に対する安全性評価と、その対策が練られる必要がある。

d) エンドユーザが安心できるバイオメトリクス
・新しい技術を利用し始める際には、新しい脅威に対する備えをしておく必要がある。
⇒「身体的特徴の偽造による攻撃」に対する対策は？
⇒ ①脆弱性を評価する手法の確立、
②生体検知機能の導入、
③未知なる脆弱性を発見し、対応する体制整備
・エンドユーザが、「高度なセキュリティ技術」と信じ、高いリスクを委ねようとする技術である程、エンドユーザに対して、その技術の安全性を説明し、信任を得ていくことが大切である。

３）銀行におけるバイオメトリクスの実用化[7]

a) バイオメトリクス（生体認証）

・認証技術の進歩

・ ユビキタス・ネットワーク社会の到来

9.11 同時多発テロを契機として、本人確認手段として注目

・クローズドからオープン環境での実用化

b) 検討項目

・どの方式を採用するか

・利用チャネル

・操作性

・精度評価の問題

FRR（本人拒否率）と FAR（他人受入率）

評価方法、評価対象、サンプル数、適応率 etc.

・生体認証情報の保管

プライバシ保護

・利用者の意向

c) 生体認証情報の位置づけ

・生体認証は、本人確認の手段としてのみ活用する

・生体認証情報は、個人情報のなかでも特に取扱いに慎重を要する（超）センシティブ情報

身体の特徴情報で取り替え不能（変更ができない）

d) 生体認証情報の取得

・生体認証情報は銀行では保有しない

・（超）センシティブな個人情報

・従業員の生体認証情報へのアクセス回避

・漏洩リスクの回避

・IC カードの IC チップ内に保管する

・照合処理も IC チップ内で行なう（MOC 方式）

・IC チップは堅牢なセキュリティを有する

・特徴化した情報のみ保管

・登録情報から生体情報の復元は困難

e) 利用者アンケート調査

・生体認証情報の保管（銀行 or IC カード）

・「どちらも抵抗なし」が約 6 割を占める

・「IC カードに登録」は約 1 割、「銀行が保有」は約 4 割が抵抗を感じる

（４）まとめ

現状では、バイオメトリック製品の脆弱性関連情報流通体制が確立されていないため、発見者が知

り得た脆弱性情報を適切に公表する機会が無かった。このため、発見者が技術者倫理に則って発表を行っても、一般利用者や製品開発者にとって必ずしも公開すべきでない情報も流出する可能性があった。

パネル討論においては、発見者、受付機関、調整機関、製品開発者および運用者間で脆弱性情報の取り扱いに関する行動指針の明確化が必要であることを確認した。すなわち、発見者は、知り得た脆弱性情報を放置もしくは第三者に暴露することなく、受付機関（注２）に報告する。受付機関は、調整機関（注３）に脆弱性関連情報を通知し、調整機関は製品開発者と協議したうえで脆弱性の公表時期と内容を決定する。以上の情報流通体制を学会、産業界、政府機関で詳細に協議して構築するとともに、法的な根拠を明らかにし、かつ一般利用者に対して啓発活動を続けていくことが肝要である。

さらにこうした体系にもとで、研究者、技術者は事実を追求する立場で脆弱性に関する検討を行う必要があり、学会の場ではこうした活動を支援すべきである。

注１：文献[8]によれば、専門家とは①高い専門性を持つこと、②広い裁量を持つこと、③専門家集団を作っていること、④高い社会的身分を有していること、という４つの条件がある。専門家集団である学会を中心として産学官相互に影響力のあるガイドラインに関する議論を深めるのは意味がある。
注２：ソフトウエア製品の脆弱性関連情報流通体制では、IPA が対応する。
注３：ソフトウエア製品の脆弱性関連情報流通体制では、JPCERT/CC が対応する。

[参考文献]

[1]http://www.ieice.org/jpn/about/code.html
[2]辻井、笠原：“情報セキュリティ”,昭晃堂，pp.178-183（2003.10）.
[3]早貸：“脆弱性情報の取り扱いについて”，情報処理，Vol.46，No.6，pp.662-671（2005.6）.
[4]瀬戸：“バイオメトリクスの脅威及び脆弱性公開におけるガイドライン”，第５回 BS 研究会予稿集，pp.29-36（2005.9）.
[5]鷲見：“バイオメトリクス個人認証の脆弱性保護技術”，第５回 BS 研究会予稿集，
[6]岩下：“金融業務とバイオメトリクス”，第５回 BS 研究会予稿集，pp.65-66（2005.9）.
[7]嶋田：“東京三菱銀行におけるバイオメトリクスの実用化”，第５回 BS 研究会予稿集，pp.67-69（2005.9）.
[8]名和：“インターネットと倫理感”，bit，vol.29，no.10，pp.4-26（1997.10）.

３．３　付録

３．３．１　ISO/IEC ＣＤ1 19792

Contents Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19792 was prepared by Technical Committee ISO/TC JTC1, *Information Technology*, Subcommittee SC 27, *Security Techniques*.

***Editors' Note:** Subdivision of the project into two parts as shown below does not yet have a formal status but is only a proposal as outlined in SC 27 N4927 at the moment. The proposed subdivision is as follows:*
ISO/IEC 19792 Security evaluation of biometrics

- *Part 1: Evaluation concept*
- *Part 2: Evaluation methodology for ISO/IEC 15408*

Once this proposal is approved by SC 27 the hereby attached document would then become ISO/IEC 19792-1 -- Security evaluation of biometrics -- Part 1: Evaluation concept.
This Editors' note is not a part of this document.

Information technology — Security techniques — Security evaluation of biometrics

1 Scope

This International Standard (IS) – Security Evaluation of Biometrics - specifies the specific aspects which shall be considered during each security evaluation of a biometric product and is organized in two parts:

The first part 19795-1 specifies the generic aspects which shall be considered during each evaluation process of a biometric product. It thereby only addresses aspects which are specific to the biometric technology and does not address aspects which are common to all security evaluations. Furthermore part 1 is independent from any specific evaluation methodology.

The second part of this standard 19795-2 describes how the requirements which are defined in part 1 shall be applied during evaluations according to ISO 15408 ([3])

This first part of this International Standard follows the following structure:

- Clause 4 and 5 of this International Standard give an overview of all used terms, definitions and abbreviations before clause 5 describes the core part of this IS which can be separated into four parts.
- The first part of clause 6 introduces general aspects for each security evaluation of biometrics. This includes the introduction of a concept to evaluate biometric technology on different levels.
- The second part of clause 6 describes statistical aspects of security related error rates.
- The third part of clause 6 deals with the vulnerability assessment of biometric technology before the last part describes the evaluation of aspects of privacy.

With this structure this International Standard pays attention to all special aspects which shall be considered during a security evaluation of a biometric product.

This International Standard addresses evaluators of biometric technology as well as vendors of biometric products. For evaluators this International Standard provides guidance, how to handle the technology specific characteristics of biometric technology during an evaluation while for vendors it provides guidelines which aspects of their products are important in terms of security and what needs to be provided for a security evaluation.

Because some questions of performance and generic technology aspects are important for each security evaluation process of a biometric product, some parts of this International Standard overlap with standards in ISO/IEC TC JTC1/SC 37. But as this International Standard is focused on security evaluation these aspects have been adapted to be used in security evaluations.

2 Conformance

To conform to this part of ISO/IEC 19795, a security evaluation of biometrics shall be planned, executed and reported in accordance with the mandatory requirements contained herein.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19795-1 - Biometric Performance Testing and Reporting — Part 1: Principles and Framework (FDIS)

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

4.1 Terms and definitions regarding General concepts

biometrics
Automated recognition of individuals based on their behavioural and biological characteristics ([2])

biometric product
any biometric component, system or application which is the scope of the evaluation.

biometric characteristics
distinguishing trait of an individual's biology and behaviour that can be repeatably observed or measured ([2])

end-user
A person who interacts with a biometric product to enrol or have his/her identity checked. (based on [7])

wolf
A wolf is a biometric sample that shows high similarity to most of the enrolment data record

lamb
A lamb is a biometric reference that shows high similarity to most of the biometric samples from other end-users.

4.2 Terms and definitions regarding Biometric products

biometric data
biometric sample at any stage of processing, biometric reference, biometric feature or biometric property. All kinds of data related to biometric characteristics. ([2])

biometric feature
Concise representation of information extracted from an acquired or intermediate biometric sample by applying a mathematical transformation. ([2])

biometric reference
one or more stored biometric samples or biometric models attributed to an individual and used for comparison ([2])

Note: biometric template is regarded as a type of biometric reference. See definition for biometric template

biometric sample
data obtained from a biometric device, either directly or after processing ([2])

biometric template
biometric reference consisting of a set of stored biometric features comparable directly to biometric features of a presented biometric sample using a function not dependent on an individual ([2])

biometric model
biometric reference consisting of a stored function (dependent on the individual) generated from a biometric sample(s) ([2])

enrolment data record
record created upon enrolment, associated with an individual and including biometric reference(s) and typically non-biometric data ([2])

4.3 Terms and definitions regarding biometric processes

threshold
boundary value of the score used by the comparison application to decide automatically if one reference template, compared to the template submitted to the system, is accepted or rejected. ([7])

verification
biometric product function that performs a one-to-one comparison (based on[2])

identification
biometric product function that performs a one-to-many search (based on [2])

enrolment
process of creating and storing, for an individual, a data record containing biometric and, typically, non-biometric data ([2])

comparison score
numerical value (or set of values) resulting from a comparison ([2])

comparison result
value of "match", "non-match" or possibly "undetermined" resulting from a decision based on a comparison score, a decision policy including threshold, and possibly other inputs

biometric application decision
making a conclusion or resolution based on the application (3.5.1) decision policy after consideration of one or more comparison results, comparison scores and possibly other non-biometric data ([2])

4.4 Terms and definitions regarding Error Rates

failure-to-enrol rate (FTE)
proportion of the population for whom the system fails to complete the enrolment process

failure-to-acquire rate (FTA)
proportion of verification or identification attempts for which the system fails to capture or locate an image or signal of sufficient quality

false non-match rate (FNMR)
proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample

false match rate (FMR)
proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template

false reject rate (FRR)
proportion of verification transactions with truthful claims of identity that are incorrectly denied

false accept rate (FAR)
proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed

It should be noted that within [4] a FAR is defined for Zero-Effort impostor attacks only. For active impostors there are a variety of attack types, some being modality specific.

For each attack type a statistical test metric FAR_a could be computed using the mathematical formulation parallel to the definition used in [4]. There maybe several such parallel sub-tests possibly with different sizes.

$$\mathrm{FAR}_a = \frac{\text{Number of successful transactions using attack method 'a'}}{\text{Number of attacks using attack method 'a'}}$$

This kind of error rate is not considered within this clause but within the vulnerability assessment as it represents the chance to succeed with a certain kind of attack.

(true-positive) identification rate (TPIR)
proportion of identification transactions by users enrolled in the system in which the user's correct identifier is among those returned

false-negative identification-error rate (FNIR)
proportion of identification transactions by users enrolled in the system in which the user's correct identifier is not among those returned

false-positive identification-error rate (FPIR)
proportion of identification transactions by users not enrolled in the system, where an identifier is returned

target population
population users which use a biometric application.

test subject
user whose biometric data is intended to be enrolled or compared as part of the evaluation ([2])

crew
set of test subjects gathered for an evaluation ([2])

4.5 Statistical Terms

Confidence Interval
A lower estimate L and an upper estimate U for a parameter x such that the probability of the true value of x being between L and U is the stated value Y. Y is also called confidence value. (based on [4])

Confidence value
Probability that the true value for an estimated parameter x is within a certain interval.

5 Symbols (and abbreviated terms)

FAR	false accept rate
FDIS	Final Draft International Standard
FMR	false match rate
FNIR	false-negative identification-error rate
FNMR	false non-match rate

FPIR	false-positive identification-error rate
FRR	false reject rate
FTA	failure-to-acquire rate
FTE	failure-to-enrol rate
IS	International Standard
ROC	receiver operating characteristic
SDK	Software development kit
TPIR	(true-positive) identification rate

6 Security evaluation

6.1 Introduction

This clause of 19792 provides generic requirements and guidelines for a security evaluation process of a biometric product. This subclause introduces the basic concept for each security evaluation of a biometric product.

A security evaluation of biometric technology can be performed on three levels: component, system and application:

- A Biometric Algorithm as the core part of each biometric product can be tested in isolation. A **Component level evaluation** is focused on technical interfaces and biometric algorithms.
- The Implementation of a **Biometric System** can be tested in a laboratory environment. Evaluation on this level always includes a biometric sensor device and the mandatory technical equipment (e.g. a database) but is performed in a controlled laboratory environment.
- Finally a biometric product can also be evaluated on an **Application Level** which means to test the biometric system during its working in a real world environment.

As every level for evaluation has a slightly different scope and its advantages and disadvantages the following subclauses introduce the different levels in more detail.

6.1.1 Component Level

At the component level, the main scope of the evaluation are the statistical properties of the algorithm. Tests shall be performed to verify that the algorithm is accurate enough in the biometric sample discrimination on a sufficient large and representative set of tests. A test of error rates on a component level is usually a technical (off-line) test using biometric data which has been previously acquired.

Evaluation of some specific vulnerabilities shall also a part of each evaluation on a compoent level

The principal advantage of component level evaluation is the fact that such an evaluation can be controlled and documented quite easy, and it is hence repeatable and reproducible.

6.1.2 System Level

At system level, the scope of the tests and evaluation focus on the implementation of the biometric processes. Such an evaluation is typically performed within a laboratory environment but using a complete system and real users. Also on the system level the security relevant error rates shall be determined.

The test on this level is quite realistic as it includes a complete system, a simulated environment and the human factor. But nevertheless as it is performed within a laboratory it is quite good to control the environmental and operational conditions, to document the test and hence the test is quite repeatable and reproducible.

Evaluation of some specific vulnerabilities and privacy aspects shall also a part of each evaluation on a system level. The vulnerabilities which have to be additionally considered (compared to the component level) on this level include those associated with the sensor and the sensor connection.

6.1.3 Application Level

At the application level, the scope of the tests shall be the evaluation of the adequacy of the biometric product considering under real operational conditions.

This usually means that testing is done with real users and based on their normal interactions with the operational biometric system. Although such a test is realistic, it is often difficult to capture all the necessary test data to allow a comprehensive analysis of the system performance. Furthermore, the test results may not be readily repeatable because of uncontrollable changes in the test conditions.

On an application level a test shall be performed to evaluate the values for the security relevant error rates.

Some of the vulnerabilities of biometric technology have to be considered on an application level. Specifically all vulnerabilities that are related to management aspects of a biometric product (such as a de-enrolment function) or to environmental conditions (such as increasing the FAR by changing environmental factors) shall be considered on this level.

Additionally privacy aspects have to be considered on an application level as these aspects are usually application specific.

The following table summarized the advantages and disadvantages of every evaluation level in terms of the level of realism, the level of control, the cost, the time effort, repeatability and reproducibility.

	Component Level	System Level	Application Level
Level of realism	Low	Medium	High
Level of control	High	Medium	Low
Cost	Low	Medium	High
Time effort	Low	Medium	High
Repeatability	High	Medium	Low
Reproducibility	High	Medium	Low

Table 1: Advantages and disadvantages of the different levels of evaluation

6.1.4 Selection of the appropriate evaluation level

On which level a security evaluation or parts of it should be carried out is of course highly dependent on the type of the biometric product. For example it is obvious that if the product only comprises a biometric algorithm

(maybe in form of a Software Development Kit (SDK)) it can only be tested as a component because neither a system nor an application are available.

Additionally some aspects of a security evaluation may only be evaluated on a certain level. E.g. evaluation of privacy aspects is only possible in the context of a complete application. However the requirements within the rest of this standard shall be applied on all levels of evaluation if not mentioned otherwise.

However as every level of evaluation has its own advantages and disadvantages the aim shall be to evaluate the product on as many levels as possible. This means that if the product is a complete application, the evaluation shall be carried out on an application level, a system level and a component level. If the product is a biometric system the evaluation shall be carried out on a system level and a component level.

This of course means that effort has to be paid to extract a system for evaluation out of an application or to extract the core biometric component out of a system for evaluation.

The evaluation on the different levels of evaluation (where existing) shall not be seen independently. The evaluator shall examine that the results from the different levels of evaluation contribute to a homogenous result of the complete evaluation. Where inhomogeneous results exist for one aspect (or related aspects) of evaluation on different levels a justification shall be given.

6.2 Error rates of biometric products

It is one inherent disadvantage of biometric products that they do not work deterministically but have error rates which for example show how many users are wrongfully accepted or rejected by the biometric product. These error rates are not only a performance measures but are also relevant in terms of security.

Hence each security evaluation of a biometric product shall include an assessment of the security relevant error rates.

As described in clause 6.1.4 every evaluation of a biometric product shall be performed on as many evaluation levels as possible. This is also the case for the test of the security relevant error rates of the biometric product. This means that if a biometric application is the scope for the evaluation the security relevant error rates shall be tested on the system and component level as well. If a biometric system is the scope for the evaluation the test of security relevant error rates shall be performed on a component level as well. Clause 6.2.14 defines the requirements to check the consistency of the test results.

The requirements in this clause are in effect for all evaluation levels if not stated otherwise.

6.2.1 Concept

During a classical performance test of a biometric product it is usually the scope of the test to determine the error rates of a biometric product. In contradiction to this it is the scope of a test of the security relevant error rates during a security evaluation to determine whether the error rates of the biometric product are small enough to meet the security needs which are the background for the evaluation.

Hence the test of the security relevant error rates during a security evaluation starts with a claim about the behaviour of the biometric product and ends with a result showing whether this claim could be proofed during the tests or not. However the evaluator should consider some other aspects during the tests as parts of the test may be related to the vulnerability assessment as well.

As testing of error rates of a biometric product is a complex task it can usually not be done without the support of the vendor of the product. The approach for testing described in this clause bases on a five step concept:

1) The vendor shall claim the maximum values for the security relevant error rates

2) The claims shall be checked by the evaluator

3) The vendor shall perform a test to proof that the claim is correct, i.e. that the error rates meet the claim

4) The test of the vendor shall be evaluated by the evaluator

5) The evaluator shall perform an independent test

These steps will be introduced in more detail in the following paragraphs:

6.2.2 Vendor claim

The vendor of the biometric product shall provide the evaluator with a claim for the maximum value of the security relevant error rates of the biometric product.

This requirement comprises two aspects:

— The vendor shall perform and provide an analysis which error rates of the biometric product are security relevant

— The vendor shall provide the evaluator with a claim for the maximum values of these error rates.

The evaluator shall examine whether the list of security relevant error rates is complete and whether the claim for the maximum values of the error rates is adequate.

Many factors influence the decision whether the claim for the maximum values of error rates is adequate. They mainly comprise:

— The (future) application case of the biometric product and its security needs

— Legal requirements

— Contractual requirements (or customers requirements)

— Requirements resulting from the specific evaluation methodology which is used.

The evaluator shall consider at least the following error rates during the analysis to evaluate whether the list of identified security relevant error rates is complete:

6.2.3 Error rates to be considered during a security evaluation

The definition of the following error rates has been taken from [4]. Additional guidance is given for which cases the different error rates may be important.

6.2.3.1 failure-to-enrol rate (FTE)

proportion of the population for whom the system fails to complete the enrolment process

This error rate should be considered if no fallback system for the biometric product is available which could be used by the people who are not able to enrol into the biometric product.

6.2.3.2 failure-to-acquire rate (FTA)

proportion of verification or identification attempts for which the system fails to capture or locate an image or signal of sufficient quality

6.2.3.3 false non-match rate (FNMR)

proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample

6.2.3.4 false match rate (FMR)

proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template

6.2.3.5 false reject rate (FRR)

proportion of verification transactions with truthful claims of identity that are incorrectly denied

6.2.3.6 false accept rate (FAR)

proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed

It should be noted that within [4] a FAR is defined for Zero-Effort impostor attacks only. For active impostors there are a variety of attack types, some being modality specific.

For each attack type a statistical test metric FAR_a could be computed using the mathematical formulation equivalent to the definition used in [4]. There could be several such sub-tests possibly with different sizes.

$$FAR_a = \frac{\text{Number of successful transactions using attack method 'a'}}{\text{Number of attacks using attack method 'a'}}$$

This kind of error rate is not considered within this clause but within the vulnerability assessment as it represents the chance to succeed with a certain kind of attack.

The FAR shall be considered during each evaluation of a biometric verification product.

6.2.3.7 (true-positive) identification rate (TPIR)

proportion of identification transactions by users enrolled in the system in which the user's correct identifier is among those returned

This error rate should be considered during an evaluation of a biometric identification product.

6.2.3.8 false-negative identification-error rate (FNIR)

proportion of identification transactions by users enrolled in the system in which the user's correct identifier is not among those returned

This error rate should be considered during an evaluation of a biometric identification product.

6.2.3.9 false-positive identification-error rate (FPIR)

proportion of identification transactions by users not enrolled in the system, where an identifier is returned

This error rate should be considered during an evaluation of a biometric identification product.

6.2.4 Vendor test

The vendor shall plan and conduct a test with the aim to proof whether the error rates meet the claim. This test shall be compliant to 19795-1.

19795-1 defines the requirements for performance testing of biometric products and should therefore be followed. In contradiction to many classical performance tests as described in 19795-1 it is the scope of a test of the security relevant error rates during a security evaluation to proof a claim about the maximum values of the error rates wrong or right. Hence the rest of this clause defines additional requirements that shall also be followed. These requirements are either not contained in 19795-1 or not mandatory to be compliant to 19795-1.

The vendor of the biometric product shall provide the evaluator with the description and the results of the test performed to proof that the claim for the security relevant error rates can be met. The test shall be compliant to 19795-1 and shall meet the additional requirements as listed in the rest of this clause.

The evaluator shall examine the test and check whether it has been performed in compliance with 19795-1.

Additionally the test shall meet the requirements described in the rest of this clause which shall be checked by the evaluator.

As the efforts for such a test may be quite high it is also possible that the evaluator reviews the test concept of the vendor before the vendor conducts the tests. In this way a test which cannot be used due to an error in its concept can be avoided.

6.2.5 Assumptions

Each test of error rates of biometric products needs assumptions during its design and test phase.

The vendor shall report all assumptions which have been made for the design and conduction of the test.

Classical assumptions for example address:

— The future environment of the biometric product

— The independence of attempts to the system in a statistical sense

— The expected behaviour of future genuine users of the biometric product

— The expected behaviour of attackers which might attack the biometric product in the future

The assumptions made for the test bias the assurance which can be achieved in the results of the test.

The evaluator shall evaluate the assumptions reported by the vendor and check whether these assumptions are appropriate for the required level of assurance.

All assumptions which have been made for the design of the test or during the tests shall be documented and published together with the test results.

6.2.6 Test crew

The test crew which is acquired for evaluation shall be representative of the target population of the biometric product.

This requirement can be easily met if the test crew is collected randomly from the target population of the system.

If it cannot be shown that the test crew has been randomly collected from the target population of the biometric product the vendor shall identify the characteristics of the test crew which may bias the security relevant error rates.

Additionally the vendor shall report the distribution of the identified characteristics among the test crew and the target population of the biometric product. For evaluations on a component or system level a hypothetical target population may be assumed.

The evaluator shall examine the analysis of the vendor. This analysis shall comprise:

— An analysis whether the test crew has been randomly collected from the target population (if claimed by the vendor)

Or:

— An analysis whether the list of influencing factors claimed by the vendor is complete and

— An analysis whether the distribution of the identified characteristics among the test crew differs significantly from the distribution of these characteristics among the target population.

However it should be noted that one possible attack to a biometric product may be that an attacker uses the biometric characteristics from a user who comes from outside the target population. The question whether this would bias the security relevant error rates shall be addressed by the evaluator during the independent tests.

6.2.7 Environment

The environmental conditions which could influence the performance of the system during the test shall not deviate significantly from the recommended conditions. This requirement includes that the vendor has to define the intended environment in which the biometric product may be used if the test is performed on a component or system level.

The evaluator shall check that the environmental conditions do not significantly differ from the conditions in the intended environment.

All environmental conditions relevant to the test scenario shall be documented and published. Additionally the intended environment for the biometric product shall be published together with the evaluation results.

During the independent tests the evaluator shall specifically examine the possibility that the security relevant error rates can be increased by attacking the system by changing parameters in the environment to a value out of the recommended range. See also clause 6.3.8.

6.2.8 Related error rates

If an error rate which is determined is related to another error rate directly or indirectly the value for the related error shall to be claimed and published as well.

The evaluator shall check that the value for the related error rate is acceptable.

The background for this requirement is to avoid that a biometric product is tuned to reach a certain error rate (e.g. FAR) while the correlated error rate (e.g. FRR) reaches unacceptable values which would make the system unusable working point.

6.2.9 Threshold settings

While in classical performance testing the scope is often to calculate the complete ROC of the biometric product during a security evaluation only the behaviour of the system at its recommended settings is relevant. However if the biometric product allows to adjust the settings for the threshold all settings which are allowed shall be tested.

Even if not required it is possible to report the ROC of the biometric product.

Hence all possible threshold settings of the biometric product shall be made in accordance with the guidance documentation during testing and shall be published together with the test results.

The evaluator shall check that the threshold settings during the tests were set correctly.

6.2.10 Retry counter

Some biometric products allow sequential reject retries before the product takes defensive measures (e.g. account lockout). This is a critical aspect of the overall security.

If a biometric product has a mechanism to limit the maximum number of failed (sequential) attempts the vendor shall provide the description of this mechanism and the recommendations for its settings.

The evaluator shall examine the described mechanism and check the settings for a retry counter to be appropriate for the application case of the biometric product.

As the error rates for multiple attempts cannot be easily calculated based on the one attempt error rates, the vendor test shall report the results for the error rates considering the retry counter setting of the biometric product.

6.2.11 One attempt error rate

Some of the error rates of a biometric product may base on a multiple attempt philosophy. (See also prev. subclause) E.g. it may be the case that one single rejected genuine attempt of a user is not seen as a false rejection but only an accumulation of x rejected genuine attempts.

In these cases a vendor may tests and reports the values for an error rate of X attempts (e.g. FRR(3)).

However for the reason of comparability the value for the 1 attempt error rate shall be tested, reported and published anyway.

It should be mentioned that it is usually not possible to calculate the error rates for multiple attempts based on the one attempt error rate or vice versa. Hence in these situations both error rates have to be tested. While this is usually quite simple in a component test on a system or application level it may be necessary to collect information which is usually not collected.

6.2.12 Statistic Approach/Confidence values

The vendor shall document the statistic approach which has been used to proof the claim of the maximum values for the security relevant error rates and provide the evaluator with this information.

The evaluator shall check that the used approach is suitable.

The confidence value which has been used shall be reported to the evaluator as well and the evaluator shall check that the used confidence values are adequate for the required level of assurance.

The used statistic approach and the used confidence value shall be published together with the evaluation results.

6.2.13 Repeat test subset/Vendors testing

The concept of this standard defines that the test of the security relevant error rates is primarily performed, documented and reported by the vendor of the biometric product. However the evaluator shall perform independent tests to check the results of the vendor.

During the independent test the evaluator shall specifically address the following questions:

1) Are the results of the vendors test correct?

2) Does an accumulation of false acceptance cases exist?

3) How does a variation of the environment bias the test results?

4) How does a variation of the characteristics of the test crew which have been identified by the vendor to influence the security relevant error rates (see also clause 6.2.5) bias the test results?

5) The evaluator shall consider the typical vulnerabilities as described in clause 6.3 during the independent test.

To verify that the results of the vendor are correct it may be sufficient to repeat a subset of the test the vendor provided the evaluator with. This is specifically possible for tests on a component level. Also to evaluate the bias of a different environment or the possibility to exhaust the vulnerabilities the evaluator may reuse test data and results of the vendor's test.

However the independent test shall meet the following requirements:

1) The acquisition of the test crew/test data shall be under the sole control of the evaluator.

2) The planning and the conduction of the test shall be under the sole control of the evaluator

3) The evaluator should follow 19795-1 to plan and perform the test. However for some aspects during the independent test the evaluator will have to develop a different methodology.

6.2.14 Consistency check

If the scope of the evaluation is a biometric system or application more than one test for the security relevant error rates shall be performed as explained in clause 6.2.1.

The test on every level has to meet the requirements from the previous clauses if not explicitly stated otherwise.

If more than one level of testing has been performed (i.e. for system or application evaluations) the evaluator shall evaluate the test results of every level to show that no inconsistencies exist.

It is well known that test results of error rates of the same biometric product which are tested on different levels are not directly comparable. However the evaluator shall at least address the following questions during this analysis:

— Did all tests show that the corresponding claims for the error rates are met?

— Did all the tests identify the same security relevant error rates? If not, is justification given?

— Are there any obvious and not justifiable inconsistencies within the results of the tests?

6.3 Vulnerability Assessment

This subclause describes the requirements and recommendations concerning the vulnerability assessment of biometric products. Potential vulnerabilities that are well known are addressed in the following subclauses. Table 2 lists the potential vulnerabilities and related subclauses.

Major threats assumed this subclause are following. Concrete attack processes are described in each subclause corresponding to the potential vulnerability.

— **Intentional impersonation**: The attacker tries to exploit the potential vulnerabilities and impersonate a legitimate end-user at the verification or identification.

— **Accidental impersonation**: Due to the potential vulnerability, the end-user is accepted as another legitimate end-user at higher false accept rate than predicted one by performance testing that was carried out beforehand. It is threats for the identification or verification.

— **Creating backdoor**: To create the account at the enrolment that one or more attackers can be accepted by the biometric product.

Each subclause includes an explanation of a potential vulnerability, the requirements that vendors and evaluators shall meet to ensure the potential vulnerability cannot be easily exploited, an explanation of threats in combination with other potential vulnerabilities, and the requirements that vendors and evaluators shall meet to ensure the target system is resistant to the threats.

Although the subsystems and processes of the biometric product in this subclause are based on the general biometric product that has been defined [7], some subsystem and sub-components are also appended with regard to the security evaluation of the biometric product. These additional subsystems, sub-components and processes are described in Annex A of this document. During a security evaluation of a biometric product the evaluator shall at least consider the vulnerabilities listed in this clause.

Requirements for the assessment of vulnerabilities depend on the evaluation level. Table 2 also summarizes the requirement for each potential vulnerability according to the evaluation level. "N/A" means the evaluator does not have to assess the potential vulnerability at the evaluation level. A "Basic" assessment is to clarify the degree of a single potential vulnerability at the evaluation level. An "Extended" assessment is to confirm that the target, which can be a biometric component, system, or application, is resistant to threats related to the vulnerability. According to the basic concept for evaluation (see also clause 6), the evaluation levels form a hierarchical structure. That is, a system level evaluation shall include a component level one, and an application level evaluation shall include a system level evaluation. However, extended assessments are not required when a basic assessment shows that the potential vulnerability cannot be exploited. Therefore, it may be efficient for a system or application level evaluation to start from the component level.

Subclause	Potential Vulnerability	Component	System	Application
4.3.1	Imitation	N/A	Basic	Extended
4.3.2	Mimicry	Basic	Extended	Extended
4.3.3	Deficient liveness check	N/A	Basic	Extended
6.3.4	Impossibility of concealing biometric characteristics	N/A	Basic	Extended
6.3.5	Similarity	Basic	Extended	Extended
6.3.6	Special biometric characteristics	Basic	Extended	Extended
6.3.7	Synthesised biometric samples	Basic	Extended	Extended
6.3.8	Unexpected Environment	N/A	Basic	Extended
6.3.9	Configuration	N/A	Basic	Extended
6.3.10	Enrolment process	N/A	N/A	Basic
6.3.11	Leakage and alteration of biometric data	N/A	Basic	Extended

Table 2: Vulnerability assessment based on the three levels of evaluation

The potential vulnerabilities described in this IS are common to most biometric products but new biometric technologies or specific designs of biometric applications may have other vulnerabilities. Note that not all

vulnerabilities are covered in this document. Therefore, the evaluator shall also perform a state-of-the-art examination to reveal the existence of other vulnerabilities not described here.

6.3.1 Imitation of biometric characteristics

Biometric characteristics are not designed in a way intended to prevent their imitation, unlike other personal identification devices such as smart cards or the keys to a safe. There are biometric characteristics that would be easy for anyone to reproduce ([8], [9]). These can be reproduced by, for instance, rubber fingers or recorded voices. This is a potential vulnerability that could lead to impersonation for a biometric product, and also allow a backdoor to be created during enrolment.

To confirm that this potential vulnerability cannot be easily exploited, the vendor shall provide information concerning imitation prevention that includes the ease (or difficulty) of achieving imitation, the specification of capture- and imitation-prevention sub-components, the environmental and operational conditions assumed for the biometric product, and the claimed difficulty of achieving imitation against the biometric product. The vendor can also provide test results regarding imitation. In addition, any known limitations of effectiveness for imitation prevention shall be stated. The evaluator shall assess the imitation prevention with the aim of validating the vendor's claims. Additionally the evaluator shall use any other available spoofing techniques to assess the capability of the imitation prevention against known forms of imitations relevant to the biometric modality and technology. These requirements are in effect for the system level evaluation.

If the above evaluation leads to strong suspicion of an imitation vulnerability, the evaluator shall also assess the following threats.

One threat exploiting this vulnerability is the intentional impersonation with an artificial material that can provide a biometric sample closely resembling that of a specific person. Since original biometric samples are needed for this threat, the evaluator should also consider the ease of acquiring original biometrics to evaluate the resistance against this threat. To enable assessment of this threat, the vendor shall provide information concerning the difficulty of acquiring original biometric samples which should address at least the potential vulnerabilities described in 6.3.4 and 6.3.11. Any other countermeasures against this threat can be addressed. The vendor shall also claim whether the target system is resistant to this threat. The evaluator shall validate the vendor's claim. These requirements are in effect for the application level evaluation.

The other threat is creation of a backdoor through imitation during enrolment. If an imitation can be enrolled and verified, it may be used by anyone as a token to access the system. Since the imitation does not need to provide a legitimate end-user's biometric data for this sort of attack, no effort to acquire original biometric samples is required on the part of attackers. On the other hand, an attacker should enrol the imitation within the biometric product. Therefore, the evaluator should also consider the enrolment process to confirm the resistance to this type of attack. To enable assessment of this threat, the vendor shall provide the operational conditions of the enrolment process and claim the biometric product is resistant against this threat. For example, enrolment monitored by the staff administering the enrolment process may be an effective countermeasure. The evaluator shall validate the claim of the vendor. These requirements are in effect for the application level evaluation.

Note: Physiological biometric characteristics cut off from end-users are not considered a form of imitation (see 5.3.3.)

6.3.2 Mimicry of biometric characteristics

Biometric samples may change for many reasons. In particular, end-users may intentionally change behavioural biometric characteristics such as their voice or dynamic signatures. Mimicry refers to these kinds of intentional change of behavioural biometric characteristics. This is a potential vulnerability that could lead to the thread of impersonation and the creation of a backdoor for the biometric product.

To ensure this potential vulnerability cannot be exploited, the vendor shall provide information related to the component of the biometric product which includes the specification of the component, and the environmental and operational conditions assumed for the biometric product, and the claimed difficulty of mimicry against the biometric product. In addition, any known limitations of effectiveness against mimicry shall be stated. The evaluator shall assess the ease of mimicry with the aim of validating the vendor's claims. These requirements are in effect for the component level evaluation if behavioural biometric characteristics are employed.

If the above evaluation leads to strong suspicion of mimicry vulnerability, the evaluator shall also assess the following threats.

As for the intentional impersonation through mimicry of a legitimate end-user, the evaluator should consider the ease of acquiring original biometrics as well as confirming the resistance against this threat, since original biometric samples are needed to achieve this threat. To enable assessment of this threat, the vendor shall provide information on the difficulty of acquiring original biometric samples which should address at least the potential vulnerabilities described in 6.3.4 and 6.3.11. Any other countermeasures against this threat can be addressed. The vendor shall also claim whether the biometric product is resistant against this threat. The evaluator shall validate the vendor's claim. These requirements are in effect for the system level evaluation.

This potential vulnerability can also lead to the creation of a backdoor where end-users (and attackers) carry out training in collusion with each other to submit identical biometric characteristics such as the same keyword or the same signature. Regarding this threat, the evaluator should also consider the enrolment process. To enable assessment of this threat, the vendor shall provide the operational conditions of the enrolment process and claim that the biometric product is resistant against this threat. For example, the biometric product that does not allow end-users to decide the keyword used to enrol in the system could be a countermeasure to this threat. The evaluator shall validate the claim. These requirements are in effect for the application level evaluation.

6.3.3 Deficient liveness check

A deficient liveness check sub-component may allow impersonation or creation of a backdoor with physiological body parts cut off from the end user. The imitation prevention may not detect this attack since the submitted biometric characteristics are real, though not living, in this case.

To ensure this potential vulnerability cannot be exploited, the vendor shall provide information concerning the liveness check that includes the qualitative change in the biometric sample after being cut off, the effect of the change on capture, the specification of capture- and liveness-check sub-components, the environmental and operational conditions assumed for the biometric product, and a claim as to how long the biometric characteristics of a cut-off part can be used for verification or identification. The claim can be made from a medical perspective. No experimental testing may be possible. In addition, any known limitations on the effectiveness of the liveness check shall be stated. The evaluator shall assess the liveness check with the aim of validating the vendor's claims. These requirements are in effect for the system level evaluation when physiological biometric characteristics are employed.

If the above evaluation concludes that the biometric characteristics of a cut-off part can be used for a practical length of time, the following threats shall also be assessed by the evaluator.

Regarding intentional impersonation using the biometric characteristics of a cut-off part, the vendor shall provide the assumed social circumstances of the application or operational conditions on verification or identification, and claim how difficult it will be for attackers to obtain the biometric characteristics of a cut-off part. The evaluator shall validate the claim. These requirements are in effect for the application level evaluation.

This potential vulnerability may also lead to the creation of a backdoor if the biometric characteristics of the cut-off part can be used for long enough. Regarding this threat, the evaluator should also consider the enrolment process to confirm resistance to this attack. To enable assessment of this threat, the vendor shall provide the operational conditions for the enrolment process and claim the biometric product is resistant against this threat. For example, enrolment monitored by the staff administering the enrolment process may be an efficient countermeasure. The evaluator shall validate this claim. These requirements are in effect for the application level evaluation.

6.3.4 Impossibility of concealing biometric characteristics

Since biometric characteristics are readily exposed to others, it is difficult (not to say impossible) for end-users to always intentionally conceal their biometric characteristics. Therefore, even if countermeasures against leakage of biometric data in systems are strong enough, attackers may acquire a legitimate end-user's biometric sample. For example, it might be possible to obtain a fingerprint that has been left on the biometric

capture device, a photograph of a face or a voice recording. This is a potential vulnerability that could lead to the threat of impersonation or the threat of creation of a backdoor during enrolment for the verification or the identification system.

To confirm this potential vulnerability cannot be exploited, the vendor shall provide information concerning the biometric characteristics used in the biometric product, the specification of capture subsystem, the environmental and operational conditions assumed for the application, and the claimed difficulty of obtaining an end-user's biometric characteristics by covert operation. The evaluator shall assess this potential vulnerability with the aim of validating the vendor's claims. These requirements are in effect for the application level evaluation.

If the marks of biometric characteristics remain on the capture subsystem, the vendor shall claim how difficult it will be to abuse the marks without imitation. For example, a fingerprint on the capture subsystem might be verified again by applying appropriate moisture. The evaluator shall validate this claim. These requirements are in effect for the system level evaluation.

If the above evaluation leads to a strong suspicion that this vulnerability is significant, the evaluator shall also assess the following threats.

End-user biometric characteristics obtained by covert operation may become a resource for imitation or mimicry and may lead to intentional impersonation through imitation or mimicry. Regarding these threats, the evaluator shall also consider imitation or mimicry.

To enable assessment of these threats, the vendor shall provide information on the difficulty of imitation or mimicry that is described in 6.3.1 or 6.3.2. Any other countermeasures against these threats can be addressed. The vendor shall also claim that the target system is resistant to these threats. The evaluator shall validate the vendor's claim. These requirements are in effect for the application level evaluation.

6.3.5 Similarity

Depending on the modality of biometrics, the biometric characteristics of close blood relatives or identical twins may be very similar. Regarding facial recognition methods, for example, there is often a very strong resemblance between the facial features of blood relatives, especially siblings or twins. Such similarity may lead to the threat of intentional impersonation for verification systems, intentional or accidental impersonation for identification systems, and the creation of backdoors.

To confirm this potential vulnerability cannot be exploited, the vendor shall provide information concerning the similarity of biometric characteristics from closely related (by blood) end-users that includes the environmental and operational conditions assumed for the biometric product. The vendor shall also claim that similarity among closely related end-users can not deteriorate the false accept rate. The claim can be made from a medical perspective or by analysing false accept cases. For the analysis, the vendor should refer to subclause 6.2 The degree of this potential vulnerability can be examined through evaluation of the false accept rate under the special condition where the test subjects (crew) consist of close blood relatives or identical twins. If the conditional false accept rate greatly surpasses the false accept rate, the degree of vulnerability and related risk can be high. The evaluator shall assess this potential vulnerability with the aim of validating the claim. These requirements are in effect for the component level evaluation.

If the above evaluation shows that the similarity can deteriorate the false accept rate, the following threats shall be also assessed by the evaluator.

This potential vulnerability may lead to the threat of impersonation by attackers who are related by blood to a legitimate end-user submitting their biometric characteristics to the biometric product. The vendor shall provide information on countermeasure in the system or the application level and claim its effectiveness. The evaluator shall validate this claim. These requirements are in effect for the system or the application level evaluation.

This potential vulnerability may also lead to the threat of backdoor creation where legitimate end-users accounts are available to the end-user's close blood relatives. Regarding this type of attack, the vendor shall provide information on countermeasures at the application level and claim their effectiveness. The evaluator

shall validate this claim. These requirements are in effect for the application level evaluation. For example, checking during the enrolment process whether the end-user has an identical twin may be one countermeasure.

6.3.6 Special biometric characteristics

Biometric samples showing "special behaviour" differing from that of the usual samples are known as either a wolf or a lamb ([1]). They have similarities higher than normal samples to many impostors. The existence of such special biometric samples can lead to the threat of impersonation or backdoor creation.

To confirm this vulnerability cannot be exploited, the vendor shall provide the specification of the component and claim that the existence of a special biometric sample or references is rare. The vendor can provide the result of a false accept case analysis. In this case, the evaluator should refer to the analysis of false accept cases described in subclause 6.2. The evaluator shall assess this potential vulnerability with the aim of validating the vendor's claims. These requirements are in effect for the component level evaluation.

Note: The existence of special samples can be predicted by examining the specifications of the biometric subsystem, especially regarding the pre-processing and feature extraction sub-components, and compare subsystem. The results of performance testing are also useful for predicting the existence of such samples or reference, because a concentration of false accepts related to a specific subject will suggest the possible existence of special biometric characteristics. If the possible existence of such characteristics cannot be denied according to the specifications, the evaluator should conduct a performance test.

If the component level evaluation leads to a strong suspicion of vulnerability, the following threats shall be assessed.

The threat exploiting this potential vulnerability is that end-users who have special biometric characteristics will submit their biometric characteristics to the biometric product. That may cause intentional impersonation by attackers as well as an accidentally high false accept rate by legitimate end-users in an identification system. The vendor shall provide information on countermeasures against these threats and claim how effective they are. The evaluator shall validate the claim. These requirements are in effect for the system level evaluation.

This potential vulnerability may also lead to backdoor creation where end-users who have special biometric characteristics are enrolled as legitimate end-users. Either fortuitously or intentionally, many impostors can be verified or identified as these end-users. Since this threat makes it important to prevent the enrolment of end-users who have special biometric characteristics, the vendor shall provide information on countermeasures in the enrolment process and claim how effective they are. The evaluator shall validate the claim. These requirements are in effect for the application level evaluation.

Note: Analysis of case of false accept during enrolment can be an effective countermeasure against backdoor creation .

6.3.7 Synthesised biometric samples

Depending on the specifications of the feature extraction sub-component, the quality-control sub-component, and the compare subsystem, false accept might occur with input that is unrealistic with regard to the viable range of human biometric characteristics. Such synthetic data could possibly match one or more enrolees, giving rise to instances of false accept.

To confirm that this vulnerability cannot be exploited, the vendor shall provide the specifications of the feature extraction and the quality-control sub-component, and the compare subsystem. The vendor shall also claim that the capabilities of the quality control sub-component are sufficient to reject synthetic data, that the feature extraction sub-component will not output the significant features from synthetic data, or that the compare subsystem will not output a high similarity between synthetic data and the biometric references. The evaluator shall assess this vulnerability with the aim of validating the vendor's claim. These requirements are in effect for the component level evaluation.

If the component evaluation leads to a strong suspicion of this vulnerability, the evaluator shall also assess the following threats.

This vulnerability may lead to the threat of intentional impersonation for biometric products in which attackers submit an artificial object that provides the synthetic data. The vendor shall provide information on countermeasures and claim their effectiveness. The evaluator shall validate this claim. These requirements are in effect for the system or the application level evaluation.

This potential vulnerability may also lead to backdoor creation through which synthetic data is enrolled. Either fortuitously or intentionally, many impostors can be verified or identified as a legitimate end-user. The vendor shall provide the information on countermeasures in the enrolment process and claim how effective they are. The evaluator shall validate this claim. These requirements are in effect for the application level evaluation. For example, an efficient countermeasure may be enrolment monitored by the staff administering the enrolment process.

6.3.8 Unexpected Environment

The physical environment around the capture subsystem may affect the false accept rate. The lighting conditions for face verification, humidity for fingerprint verification, and noise for voice verification are examples of environmental conditions that may affect the false accept rate. See Annex A.4.1 "Environmental Conditions" for other examples. Deterioration of the capture subsystem, such as stains or flaws on the sensor, may also be caused by external factors that thus affect the false accept rate. On the other hand, a testing of security relevant error rates can be carried out under the physical environment that the vendor assumes or the application specifies. Therefore, a physical environment that is unexpected in the testing may increase the values of the security relevant error rates. This is a potential vulnerability that could lead to the threat of an accidentally high error rates.

To enable assessment of this threat, the vendor shall provide information on the possibility that an unexpected environment may affect the security relevant error rates. The evaluator shall assess the information with the aim of validation. These requirements are in effect for the system level evaluation.

As for the application level evaluation, the vendor shall provide information on the physical environments of the target application, and claim that no specific environment that might affect the security relevant error rates will be realized for the target application. The evaluator shall validate this claim. These requirements are in effect for the application level evaluation.

6.3.9 Configuration

Biometric verification or identification is carried out by comparing a submitted biometric sample with a biometric reference(s) and determining the match based on a decision policy. Generally, the precision level of the determining criterion is adjusted by changing the values of the parameters for the decision. A typical parameter for the verification decision is a threshold value with respect to the comparison score. There are cases in which the expected false accept rate cannot be achieved because the parameters for the verification decision have been deliberately or accidentally set to the wrong values. Biometric products have such parameters that affect the security relevant error rates; non-administrative setting of these parameters may lead to the threat of intentional impersonation or accidentally high error rates.

To confirm that this vulnerability cannot be exploited, the vendor shall provide information on all parameters that may affect the security relevant error rates and the specification of the configuration subsystem and claim that these parameters are limited to ensure the error rates are reasonably low. The evaluator shall assess this claim. These requirements are in effect for the system level evaluation.

At the application level evaluation, the vendor shall provide the operational conditions of the configuration and claim that an appropriate authentication of the administrator is prescribed for the parameter settings. The evaluator shall assess this claim. These requirements are in effect for the application level evaluation.

6.3.10 Enrolment process

The quality of biometric references may affect the security relevant error rates. If a biometric reference of insufficient quality for the compare subsystem is enrolled in the biometric product, the false accept rate will not reach the value that was predicted from performance testing. This potential vulnerability may lead to an

accidentally high error rates or intentional impersonation if attackers can specify an end-user whose reference quality is not appropriate for verification or identification.

The vendor shall therefore provide information on the means to ensure an acceptable reference quality at the enrolment process and claim how efficient it is. The means can be applied as a function of the sub-system or certain process at the enrolment. For example, FAR testing of the reference against a database of biometric samples may be an effective countermeasure to this potential vulnerability. The evaluator shall assess this claim with the aim of validation. These requirements are in effect for the application level evaluation.

Since the enrolment process provides an end-user with the privilege of access to the protected assets, the establishment of the unique identity of the end-user through non-biometric means may be mandatory for the enrolment. Proofing is typically achieved through the use of so-called "breeder documents" such as birth certificates, passports, etc. Inadequate proofing may lead to the threat of creating backdoor. The vendor shall therefore provide information on the operational conditions for proofing, and claim how effective the proofing is. The evaluator shall assess this claim. These requirements are in effect for the application level evaluation.

6.3.11 Leakage and alteration of biometric data

Leakage and alteration of security related data such as biometric samples, biometric references, comparison scores, and comparison results may lead to threat of intentional impersonation. For example, if the attacker can eavesdrop and feed a biometric sample to the cable between the capture subsystem and the signal processing subsystem, the intentional impersonation could be achieved exploiting these vulnerabilities. A variety of attack processes can be found on [1][10].

The vendor shall provide information on the security related data of the target system and countermeasures against leakage and alteration, and claim that security related data cannot leak and be altered. The evaluator shall assess this claim with the aim of validation. These requirements are in effect for the system and the application level evaluation

6.4 Privacy

Biometric products frequently associate personal information such as identity to biometric characteristics.

Furthermore, biometric characteristics or templates may contain by themselves personal information such as gender, ethnic group or age. Therefore privacy is an important issue to be considered during each security evaluation of a biometric application.

Privacy shall be granted by the prevention of unauthorized access to personal data including biometric characteristics or template.

Note: As privacy issues are often addressed by organisational means and highly dependent on a concrete usage, the evaluation of these aspects has to be done on the application level. Some of the technical means (e.g. encryption) could also be assessed on a system level as well but the evaluation of privacy aspects should always be related to a certain usage.

The list of privacy-relevant assets and the nature of their associated protections shall be defined upstream from the evaluation and provided to the evaluator as an input of the following items. The evaluation shall ensure that the defined privacy-relevant assets and protections are adequately protected and not used wrongfully or illegitimately.

Note: The definition of the privacy-relevant assets is not part of this IS but is national specific and could be the result of legislations or guidance from national bodies.

6.4.1 Assets protection

The evaluator shall ensure that the system provides an adequate mean to prevent unauthorized access to the privacy-relevant assets.

6.4.2 Application Binding

The evaluator shall check that the system provides a mean to prevent the privacy-relevant assets from being used in biometric products outside the scope of the application context.

Note: Due to the fact that many interoperable biometric products are available it may be possible that a biometric template is usable in another system than the system it was created for. This functionality needs to be defined in the application context.

6.4.3 De-enrolment

The evaluator shall check that the biometric product provides a mean to remove privacy-relevant assets related to a user from the system and with no residual information (De-enrolment).

Annex A
(informative)

Reference Model of a biometric product

A.1 General

This Annex describes the reference model of biometric products for security evaluation. The reference model is based on the general biometric product defined by [7] and includes the additional subsystems and sub-components, functions or processes for the context of this IS. See [7] for a more general view to a biometric product and its processes.

A.2 Reference Model

The following figure shows a reference model of biometric product for security evaluation that is used for this IS. Some processes, functions, sub-components, etc. are added to the general biometric product defined by [7] in terms of security evaluation. The several sub-components which are described in [7] are also explained in the following subclauses. These descriptions not only base on descriptions in [7] but have also been adapted to be focused on the security aspects of each sub-component.

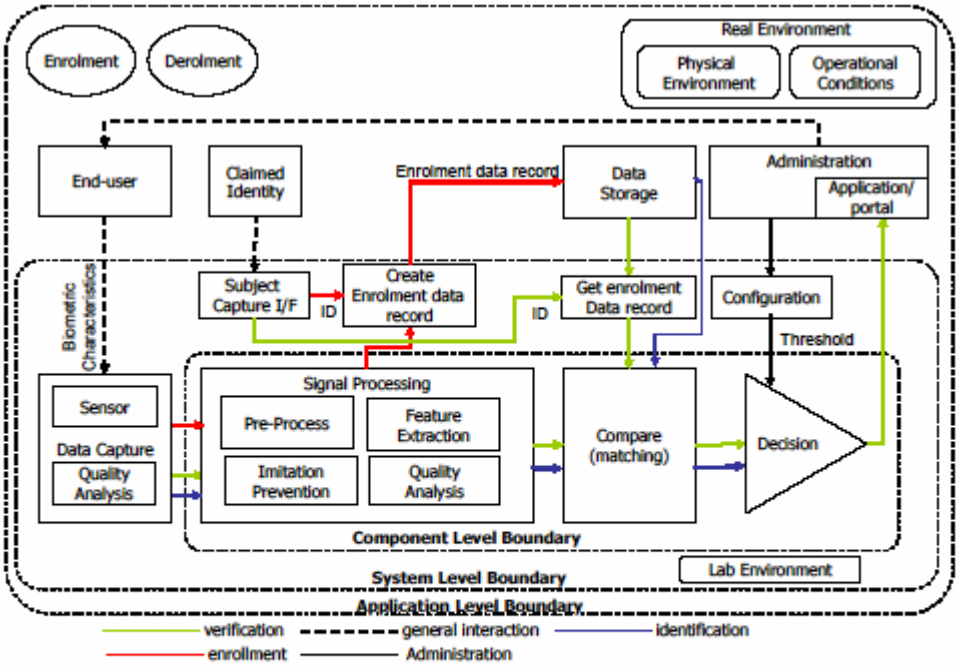


Figure 1: Generic Biometric product

A.3 Sub-Systems and sub-components

The reference model includes the sub-systems that have several sub-components in it. This subclause describes these subsystems and sub-components.

A.3.1 Data capture subsystem

This sub-system entails the acquisition of a raw biometric sample from end-user's biometric characteristics that has been presented to this sub-system. This sub-system may also include the *quality analysis* sub-component of the sample, which may result in feedback to the end-user, possibly to request that another biometric sample should be captured. The output of the capture subsystem is never a perfect representation of the raw sample, but will be affected by the characteristics of this subsystem. This sub-system also includes the *sensor* sub-component that is the technical interface to the user and may contain additional functionalities that are necessary to control the process of acquisition of the biometric sample and to interact with the user.

From a security perspective this sub-system is very important because – beside the subject Capture I/F - it is the only mandatory user visible interface. It is therefore an important interface to be considered during vulnerability analysis. Furthermore it is well known that the quality of biometric data that has been acquired by this sub-system directly influences the performance and therewith may also the security related error rates of a biometric product.

A.3.2 Signal processing subsystem

This sub-system entails the processing and conversion of the captured sample into biometric reference. This sub-system may also include quality analysis of the sample or interchange data, which may result in feedback to the end-user, possibly to request that another biometric sample should be captured. For enrolment, the data output from the signal processing subsystem is stored in the data storage subsystem. For verification, the data output from the signal processing subsystem is input to the compare subsystem.

This sub-component may include the quality analysis and the following sub-components.

A.3.2.1 Quality Analysis

This sub-component analyzes the quality of the biometric samples and the biometric references as well. This sub-component may work with one in the signal processing subsystem or be placed only in the signal processing subsystem.

A.3.2.2 Pre-Process

This sub-component entails the processing of biometric samples into the appropriate form for the feature extraction sub-component. This sub-component may include the noise reduction, image/signal enhancement, etc.

A.3.2.3 Feature Extraction

This sub-component extracts the distinguishing features out of the biometric sample. This may involve locating the signal of the subject's biometric characteristic within the received sample (also known as segmentation). This process also includes a quality analysis to ensure that the extracted features are likely to be distinguishing and repeatable. For this reason this sub-component has a connection to the capture sub-component because in case of insufficient quality it asks to acquire the biometric sample again.

A.3.2.4 Imitation prevention

The imitation prevention or liveness check is an additional security function of a biometric product. It ensures that a biometric characteristic that is presented to a biometric product really belongs to a living person and has not been faked characteristics. The imitation prevention or liveness check can be realized in many different ways. It could request a special sensor device or can be realized in software.

A.3.3 Compare subsystem

This sub-system entails the algorithmic evaluation of the similarity of the processed biometric sample with one or more of the enrolment data records. The comparison score output from compare subsystem, which is a measure of the degree of similarity, is relayed to the decision subsystem and may be relayed to the Administration sub-system for logging.

Note: Compare subsystem is described as "matching subsystem" in [7]. The definition of the "matching subsystem" appears to be inconsistent with the meaning of "matching" defined in [2].

A.3.4 Decision subsystem

This is the comparison of the score that is output from the compare subsystem with a pre-defined threshold to generate a single result of match or no match. The result is relayed to the administration subsystem for interacting with applications and may be relayed to the administration subsystem for logging.

A.3.5 Subject Capture I/F subsystem

This sub-component is the second mandatory user visible interface in a biometric product. It acquires the Claimed ID of an end-user who tries to get verified by the biometric verification system. Within the later verification process this ID is used to get the right enrolment data record out of the database and it is passed on to the environment together with the result of the verification process.

A.3.6 Get enrolment data record subsystem

This sub-system is responsible for getting the right enrolment data record out of the data storage subsystem. It has to be ensured that the communication to the storage is adequately protected and that only integer records are used for the further process. The functionality to ensure a secure communication and the integrity of used records may or may not be included in this subsystem.

A.3.7 Create enrolment data record subsystem

This subsystem entails of creating the enrolment data record of an end-user. The record is associated with the end-user via Identifier. The record will be bound to the Identifier, either by physically storing them in related locations in the data storage subsystem, or by binding them together using encryption or through a digital signature mechanism, to create an end-user record.

A.3.8 Configuration subsystem

This sub-system provides the possibility to adjust the security settings of the system. It can concern the threshold that is used for the decision subsystem; it can also concern the feature extraction tunings, and particularly the quality threshold of the features.

It also includes a mechanism that limits the ability to change the threshold setting to an administrator. Note that the authentication of the administrator must not be done via the biometric verification process but using another technique (for example a username/password based mechanism).

A.3.9 Administration subsystem

This sub-system is defined by [7] as following:

The Administration sub-system governs the overall policy, implementation and usage of the biometric product, in accordance with the relevant legal, jurisdictional and societal constraints and requirements. Illustrative examples include:

— Providing feedback to the Subject

— Requesting additional information from the Subject

— Storage and format of the Biometric Interchange Data

— Provide final arbitration on output from Verification Decision and/or comparison scores

— Set threshold

— Set biometric product acquisition settings

— Operational environment, Non-biometric data storage

— Providing appropriate safeguards for end-user privacy

— Interacting with Application that utilizes the Biometric product

A.3.10 Data storage subsystem

This sub-system is defined by [7] as follows:

The Biometric Interchange Data may be stored within a biometric capture device; on a portable medium such as a smart card, locally such as on a personal computer, or in a database.

A.4 Biometric Functions

The following subclauses introduce the basic biometric functions of a verification system. These descriptions not only base on descriptions in [7] but also have been adapted to be focused on the security aspects of each sub-component.

A.4.1 Enrolment

In enrolment, a transaction by a subject is processed by the system in order to generate and store a biometric reference for that individual.

Enrolment typically involves:

— acquiring a raw biometric sample from the Subject,

— aliveness check, preprocessing, feature extraction,

— quality analysis, (which may reject the sample/features as being unsuitable for creating a template, and require acquisition of further samples),

— biometric reference creation (which may require features from multiple samples and a end-user's ID),

Note: During enrolment the ID of the end-user is linked to his/her biometric data in form of a biometric reference. It is therefore necessary that the enrolment process of each user is controlled to ensure that the user claims his correct identity. Without this essential pre-requisite, there can be no assurance of the integrity of the enrolment database. This process is called proofing and not included in the enrolment process but the operational condition described in A.5.

A.4.2 De-Enrollment

De-Enrolment means the deletion of the biometric reference on the storage and all related biometric data in the biometric product

A.4.3 Verification

In verification, a transaction by a subject is processed by the system in order to verify a positive specific claim about the end-user's enrolment (e.g. "I am enrolled as subject X"). Verification will either accept or reject the claim. The verification is considered to be erroneous if either a false claim is accepted (false accept) or a true claim is rejected (false reject). Note that some biometric products will allow a single end-user to enrol more than one biometric sample (for example, an iris system may allow end-users to enrol both iris images, while a fingerprint system may have end-users enrol two or more fingers as backup, in case one finger gets damaged)

The verification process typically involves:

— acquiring a raw biometric sample from the Subject,

— aliveness check, pre-processing, feature extraction,

— quality checks, (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),

— Converting the captured sample into Biometric Interchange Data,

— Evaluating the similarity of the Processed biometric sample with one or more of the previously stored Biometric Interchange Data Records.

— Deciding whether the Subject matches the data represented by one or more of the previously stored Biometric Interchange Data Records.

— Interacting with the Application that utilizes the Biometric product through the Administration sub-component.

A.5 Environmental and Operational conditions of a biometric product

A.5.1 Environmental Condition

The physical environment around the capture sub-component is included in the application level as one of the items that should be evaluated. The lighting for the face verification or the humidity for the fingerprint verification is taken for instance.

The environmental condition in the application level is real and uncontrollable, because the application level evaluation focuses on the system that is operating actually. On the other hand, the system level evaluation assumes that the system is operated in laboratory or controllable environment.

Note: It is well known that environmental factors as lighting or weather may influence the performance of a biometric product. Also if performance testing is not part of this IS, it is important to consider different environmental factors at least during testing the error rates and during the vulnerability analysis. Two main reasons exists:

1) To keep an evaluation of error rates as comparable as possible to other evaluations, a detailed description of all environmental factors during the test is needed

2) It has to be considered whether certain environmental factors can lead to a lower FAR. This question is also addressed in subclause 6.3

The influencing factors of course depend on the used biometric technology. For example a voice verification system should not be influenced by different lightning while a face recognition system should not be influenced by acoustic noise. Therefore the influencing factors have to be determined for each system before an evaluation starts.

In general the factors influencing the performance an therewith the security of a biometric product can be divided into factors of the physical environment and factors regarding the users of the biometric product.

The following table which is based on [1] provides a basic overview of the influencing factors in the physical environment for selected biometric technologies. But of course this table cannot provide a complete overview but should only be seen as a base to identify the influencing factors.

	Iris	Face	Finger print	Hand	Voice
Ambient lighting	X	X	X*	X	
Ambient sound levels					X
Temperature			X	X	
Ambient electromagnetic noise	X	X	X	X	X
Atmospheric humidity			X		
Dust and other specific atmospheric contaminants	X	X	X	X	
Voltage supply variations	X	X	X	X	X
Shock and Vibration	X	X	X	X	

Table 3: Influencing factors in the environment (* not applicable to CMOS sensors)

As user related factors at least the following aspects have to be considered:

— Classical demographic factors (such as sex, age, …)

— All physiological factors that may influence the appearance of the biometric characteristic (e.g. a beard for a face recognition application)

Annex C of [1] provides a more detailed list of influencing factors and should be considered.

A.5.2 Operational Condition

The operational conditions of the enrolment and the De-Enrolment processes and the administration sub-component are included the application level as the items that should be evaluated. The proofing is also one of the operational conditions.

In terms of security, the following operational conditions are important

— How to provide an administrator with the privilege to enrol users.

— How to provide an administrator or a user with the privilege to de-enroll a biometric reference.

— How to provide an administrator with the privilege to set the parameters of the verification system.

— How to ensure that the submitted biometric characteristics are not artificial materials.

— How to ensure that the physical identities of the end-users are valid.

Bibliography

[1] *Biometric Evaluation Methodology Supplement for Common Criteria*, Version 1.0, 08-01-2002, Common Criteria Biometric Evaluation Methodology Working Group

[2] JTC 1/SC 37 Standing Document 2 - *Harmonized Biometric Vocabulary*, ISO/IEC JTC 1/SC 37 N460, 22-08-2005

[3] Common Criteria for Information Technology Security Evaluation, version 2.2, revision 256 January 2004
Part 1: Introduction and general model, CCIMB2004-01-001,
Part 2: Security functional requirements, CCIMB2004-01-002,
Part 3: Security Assurance Requirements, CCIMB2004-01-003

[4] Text of Working Draft 19795-1, Biometric Performance Testing and Reporting - Part 1: Test Principles, ISO/IEC JTC 1/SC 37 N457

[5] Text of Base Working Draft 19795-2, Biometric Performance Testing and Reporting Part 2: Testing Methodologies, ISO/IEC JTC 1/SC 37 N489

[6] ISO/IEC FCD 19784-1 Information technology -- Biometric application programme interface -- Part 1: BioAPI specification

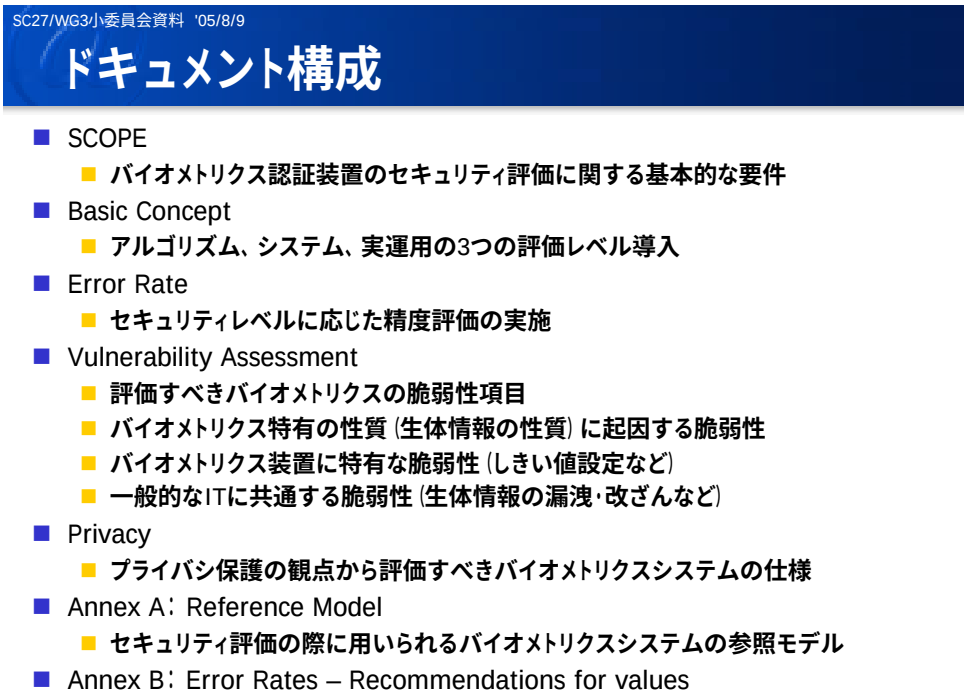
[7] ISO/IEC CD 24713-1 Biometric Profiles for Interoperability and Data Interchange -- Part 1: Biometric Reference Architecture

[8] T. Matsumoto et al., "Impact of Artificial gummy fingers on fingerprint systems," proc. SPIE Optical Security and Counterfeit Deterrence Techniques IV, 2002

[9] Ton van der Putte and Jeroen Keuning, "Biometrical fingerprint recognition : Don't get your fingers burned," Smart card research and advanced applications IFIP TC8/WG8.8, pp. 289-303, 2002

[10] C. Soutar, "Biometric System Security," Secure No.5, 2002, pp.46-49

３．３．２　SC27/WG3 国内委員会レビュー用資料



SC27/WG3小委員会資料 '05/8/9

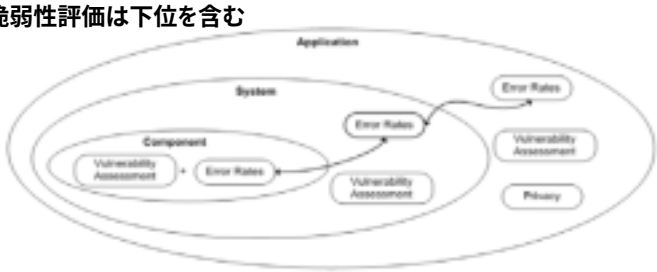
Scope

- バイオメトリクスのセキュリティ評価における要件を示す
  - バイオメトリクスに特有の問題にフォーカス
- バイオメトリクス認証 (verification) システムに特化
  - Positive Identification (識別) やNegative Identification (ブラックリストサーチ) はスコープ外
  - Identificationのセキュリティ評価はVerificationと大きく異なると予想
- SC37とのオーバーラップ
  - 用語 (SC37 SD2)、バイオメトリクスシステムの参照モデル (CD 24713)、精度評価方法 (FCD 19795) はすでにSC37で規格化が進行中
  - 19792ではSC37標準に加え、セキュリティ評価の観点を追加

SC27/WG3小委員会資料 '05/8/9

Basic Concept

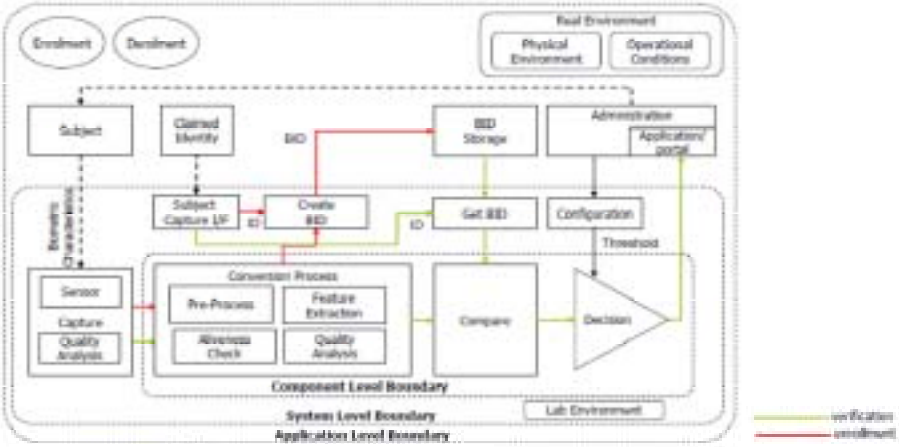
- 評価の対象・目的に合わせたセキュリティ評価レベルの導入
  - 認証精度は環境 (物理環境・利用者・運用) に影響される
  - 脆弱性は評価の対象に依存する
- Component Level
  - 認証アルゴリズムの評価
- System Level
  - 制御可能な環境下 (物理環境・利用者) における認証システムの評価
- Application Level
  - 実運用システムの評価 (制御不可能な環境下)
- レベル間の関係
  - 精度評価は各レベルでの精度の妥当性検証に用いられる
  - 脆弱性評価は下位を含む



SC27/WG3小委員会資料 '05/8/9

Annex A：Reference Model of a biometric system

- System Level
  - センサー，ユーザI/F，設定機能，制御可能な環境（物理環境・運用）
- Application Level
  - ユーザ，ストレージ，実環境（物理環境・運用），プライバシ問題，登録・削除



SC27/WG3小委員会資料 '05/8/9

Error Rate

- セキュリティに関係する精度（他人受入率：FAR）の評価
  - バイオメトリクス認証システムは代替手段を持つと想定．FRRはスコープ外．
- False Acceptanceの原因分析の実施
  - 脆弱性分析の手がかりとなる重要な情報が含まれる
- 関連する精度（FRR・FTE・FTA）の妥当性検証
  - FRRその他の評価自体が目的ではない．要求されるFARを実現するために非現実的なFRRを引き起こす可能性を排除することが目的
- 異なる評価レベル間での精度評価結果に矛盾がないことを確認
  - 評価レベル間での精度の大幅な乖離は，システム設計の誤りを示唆する
- 精度の信頼区間は要求される保証のレベルを満たす
  - 高い保証レベルを実現するには，精度の信頼区間を小さくする必要がある．SC37における精度評価では信頼度95%に固定．
- ベンダによる精度評価の方法および結果の妥当性検証．独立した小規模な追試験の実施．
  - 基本的に精度評価は評価者が実施すべきであるが，現実的に実施が困難な場合に適用される．

SC27/WG3小委員会資料 '05/8/9

Vulnerability Assessment

- 脆弱性：他人受入を頻発させる可能性のあるバイオメトリクスシステムの性質
- 本節に記載された脆弱性を評価レベルにしたがって評価
  - 記載されていない脆弱性の存在についても検討
- 生体情報の特性に依存する脆弱性の評価
  - 生体情報の複製・ものまね，秘匿の困難性，経年変化
  - 近親者や双子などにおける類似性
- バイオメトリクス・システムの仕様に依存する脆弱性の評価
  - 多くの利用者と一致しやすい特殊な生体情報/非生体情報（コンポーネント）
  - コンポーネントの一貫性（コンポーネント）
  - 生体検知，センサの性能劣化（システム）
  - テンプレートの品質管理，制限のないパラメータ設定，環境変化（システム）
  - バイオメトリクスデータ・認証結果の漏洩や改ざん（システム）
  - テンプレートおよび関連する個人情報の削除機能（システム）
  - テンプレート登録のための本人確認，生体確認，アクセス制御（アプリケーション）
- その他の脆弱性
  - 精度評価に含まれない利用者（コンポーネント）

SC27/WG3小委員会資料 '05/8/9

Privacy

- 生体情報やテンプレートへの不正アクセスを防止しなければならない
  - 生体情報には意図しないプライバシ情報が含まれることがある
    - 性別，年齢，人種，健康状態，etc…
- アプリケーションレベルでは以下について評価
  - 評価者がプライバシ保護を不要と判断した場合，その根拠を示す（要件）
  - 判断がつかない場合，プライバシ保護を必要とすることを推奨
- テンプレートへの不正なアクセス防止機能の確認
- 利用者の認識なしにテンプレートが使用されるのを防止する機能の確認
- 利用者に関する情報をシステムから削除する機能の確認
- 利用者へバイオメトリクスの利用を告知する機能の確認

３．３．３　信学会 BS 研究会　発表資料

HITACHI
Inspire the Next

バイオメトリクスセキュリティ評価基準の開発

(株) 日立製作所 システム開発研究所
セキュリティ基盤技術研究センタ
三村昌弘

本研究は、(財) ニューメディア開発協会が受託した経済産業省 産業技術研究開発委託事業「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」により開発された平成16年度成果の一部について報告する。

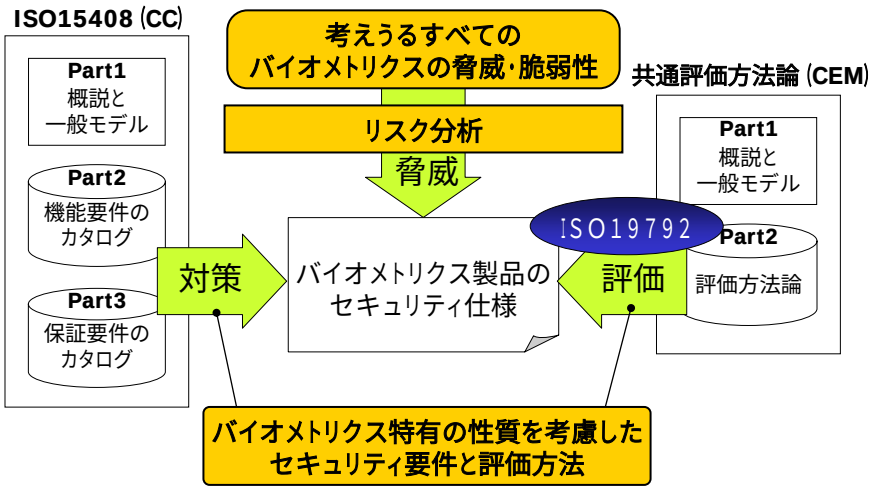
背景

- セキュリティ技術としてのバイオメトリクス
- バイオメトリクス製品の安全性とは？
  - 精度 (False Acceptance Rate：FAR)
  - 生体情報 (テンプレート) の漏洩･改ざんなど
    - IT製品としての安全性
  - バイオメトリクスに特有の脆弱性への対策
- 評価基準
  - 精度＞ISO 19795, JIS TR
  - IT製品としての安全性＞ISO 15408
  - バイオメトリクス特有の脆弱性＞？

バイオメトリクス特有の脆弱性

- バイオメトリクス特有の性質に起因する脆弱性
  - 生体情報は意識的な秘匿が困難
    - パスワードやICカードは意識的に秘匿できる
  - 生体情報を無限に作り出すことはできない
    - パスワードや秘密鍵は作り変えが可能
  - 生体情報は入力の度に変化する
  - 生体情報は個人情報のひとつである
- 脆弱性の程度がバイオメトリクス特有の脆弱性
  - 生体情報の複製の難易度
    - パスワードはコスト0，ICカードはコスト大
  - 利用者の習熟による精度の変化
  - センサ（入力装置）の劣化による精度の変化
    - 汚れなどにより比較的短期間に精度劣化を引き起こす

バイオメトリクスの安全性評価における課題



バイオメトリクスセキュリティ評価フレームワーク

- ISO/IEC JTC1 SC27/WG3
  - IT製品のセキュリティ評価標準
- ISO/IEC 19792 "A framework for security evaluation and testing of biometric technology"
- '05/8/2 4th Working Draft発行
  - コメント募集中 ('05/10末〆切)
- SCOPE
  - バイオメトリクスのセキュリティ評価における要件を示す
    - セキュリティ評価の観点から必要になる精度評価
    - 評価すべきバイオメトリクス特有の脆弱性
  - バイオメトリクス認証 (verification) システムに特化
- 想定される読者
  - 評価標準策定者，評価方法の策定者
  - 開発者 (アルゴリズム・装置・システム)

ISO/IEC 19792の概要

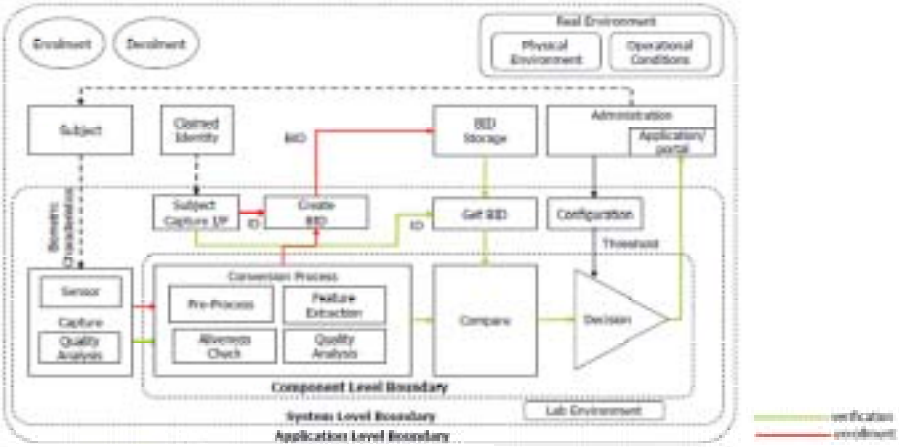
- Basic Concept
  - アルゴリズム、システム、実運用の3つの評価レベル導入
- Error Rate
  - セキュリティレベルに応じた精度評価の実施
- Vulnerability Assessment
  - 評価すべきバイオメトリクスの脆弱性項目
  - 生体情報の性質に起因する脆弱性
  - バイオメトリクス装置に特有な脆弱性 (しきい値設定など)
  - 一般的なITに共通する脆弱性 (生体情報の漏洩・改ざんなど)
- Privacy
  - プライバシ保護の観点から評価すべきシステムの仕様
- Annex A: Reference Model
  - セキュリティ評価の際に用いられるバイオメトリクスシステムの参照モデル

Basic Concept

- 評価の対象･目的に合わせたセキュリティ評価レベルの導入
  - 認証精度は環境（物理環境･利用者･運用）に影響される
  - 脆弱性は評価の対象に依存する
- Component Level ： 認証アルゴリズムの評価
- System Level ：制御可能な環境下におけるシステムの評価
- Application Level ： 実運用システムの評価

Reference Model of a biometric system

- System Level
  - センサー, ユーザI/F, 設定機能, 制御可能な環境（物理環境･運用）
- Application Level
  - ユーザ, ストレージ, 実環境（物理環境･運用）, プライバシ問題, 登録･削除



Error Rate

- セキュリティに関係する精度（他人受入率：FAR）の評価
  - バイオメトリクス認証システムは代替手段を持つと想定．FRRはスコープ外．
- False Acceptance（他人受入）の原因分析の実施
  - 脆弱性分析の手がかりとなる重要な情報が含まれる
- 異なる評価レベル間での精度評価結果に矛盾がないことを確認
  - 評価レベル間での精度の大幅な乖離は，システム設計の誤りを示唆する
- 精度の信頼区間は要求される保証のレベルを満たす
  - 高い保証レベルを実現するには，精度の信頼区間を小さくする必要がある．SC37における精度評価では信頼度95%に固定．
- ベンダによる精度評価の方法および結果の妥当性検証．独立した小規模な追試験の実施．
  - 基本的に精度評価は評価者が実施すべきであるが，現実的に実施が困難な場合に適用される．

Vulnerability Assessment

- 生体情報の特性に依存する脆弱性の評価
  - 生体情報の複製・ものまね，秘匿の困難性，経年変化
  - 近親者や双子などにおける類似性
- バイオメトリクス・システムの仕様に依存する脆弱性の評価
  - 多くの利用者と一致しやすい特殊な生体情報/非生体情報（C）
  - コンポーネントの一貫性（C）
  - 生体検知，センサの性能劣化（S）
  - テンプレートの品質管理，制限のないパラメータ設定，環境変化（S）
  - バイオメトリクスデータ・認証結果の漏洩や改ざん（S）
  - テンプレートおよび関連する個人情報の削除機能（S）
  - テンプレート登録のための本人確認，生体確認，アクセス制御（A）
- その他の脆弱性
  - 精度評価に含まれない利用者（C）

（C）：Component，（S）：System，（A）：Application

Privacy

- 生体情報やテンプレートへの不正アクセスを防止しなければならない
  - 生体情報には意図しないプライバシ情報が含まれることがある
    - 性別，年齢，人種，健康状態，etc…
- アプリケーションレベルでは以下について評価
  - 評価者がプライバシ保護を不要と判断した場合，その根拠を示す
  - 判断がつかない場合，プライバシ保護を必要とすることを推奨
- テンプレートへの不正なアクセス防止機能の確認
- 利用者の認識なしにテンプレートが使用されるのを防止する機能の確認
- 利用者に関する情報をシステムから削除する機能の確認
- 利用者へバイオメトリクスの利用を告知する機能の確認

まとめ

- バイオメトリクスの安全性評価に関する国際標準案
- バイオメトリクスの安全性評価
  - 安全性評価の観点からみた精度評価
  - バイオメトリクス特有の脆弱性への対策チェック
  - 生体情報の漏洩･改ざん防止のチェック
- ISO/IEC 19792の利用
  - 開発者：設計段階での自己評価
    - アルゴリズム開発，装置開発，システム開発
  - 評価方法策定者：最上位の要件集
    - 国際標準，各国標準，テスト機関，企業（品質保証）
- 4th Working Draftへのコメント募集中（'05/10末）