NIST Special Publication 800-76-1

個人識別情報の検証における生体認証データ仕様

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Charles Wilson
Patrick Grother
Ramaswamy Chandramouli

情 報 セ キ ュ リ テ ィ

情報技術研究所
米国国立標準技術研究所
Gaithersburg, MD 20899-8940

2007 年 1 月

米国商務省 長官
Carlos M. Gutierrez
技術管理局 技術担当商務次官
Robert C. Cresanti
米国国立標準技術研究所 所長
William Jeffrey

この文書は下記団体によって翻訳監修されています
独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
NRI SECURE TECHNOLOGIES

コンピュータシステム技術に関する報告書

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下、NIST と称する。）の情報技術ラボラトリ（ITL: Information Technology Laboratory）は、国の測定基準および標準基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。情報技術ラボラトリは、テスト、テスト技法、参照データの作成、コンセプト導入の検証、技術的分析を行い、情報技術の開発と生産的利用の拡大に努めている。情報技術ラボラトリの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティと国家安全保障にかかわらない情報のプライバシーを確保するため技術的、物理的、および管理的標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、情報システムセキュリティにおける情報技術ラボラトリの調査、ガイドライン、成果を報告し、産業界、政府機関および教育機関との共同活動についても報告する。

NIST SP 800-76-1, 33 ﾍﾟｰｼﾞ

(2007 年 1 月)

謝辞

作成者の Charles Wilson（NIST）、Patrick Grother（NIST）、および Ramaswamy Chandramouli（NIST）は、本書草稿のレビューと作成に貢献していただいた同僚に感謝の意を表する。とりわけ、連邦捜査局の手順に関する幅広い知識を提供していただいた R. Michael McCabe 氏に感謝したい。また、本書の作成に対して変わらぬ関心を寄せ、関与していただいた官民各セクター諸氏からいただいた数多くの貢献にも、心より感謝の意を表する。

本書の日本語版作成にあたっては、 産業技術大学院大学　教授　瀬戸　洋一様に、ご指導を賜りました。ここに、心より感謝の意を表します。

エグゼクティブサマリ

国土安全保障に関する大統領指令であるHSPD-12 は、連邦政府施設やシステムへの物理的および論理的なアクセスを許可するための身元証明情報の相互運用を管理する、新しい標準を採用することを要求していた。個人識別情報に関する標準を確立するために、連邦情報処理規格（FIPS 201）『Personal Identity Verification（PIV）standard for Federal Employees and Contractors』が策定された。本書（Special Publication 800-76（SP 800-76））はFIPS 201 の関連文書であり、PIVシステムでのバイオメトリクスによる証明情報の技術的な取得およびフォーマットに関する仕様を記述している。また、PIVカード [1] そのものについても記述する。指紋と顔画像の手順およびフォーマットは、公開されているバイオメトリック標準に一般的に含まれる有用性や手法に制約を加えた形で列挙した。これらの特定の仕様の主要な設計目標は、性能が高く普遍的な相互運用性である。連邦捜査局（FBI）の身元調査に適したバイオメトリックデータを用意するために、本書はFBIの文書、ANSI/NISTの『Fingerprint Standard and the Electronic Fingerprint Transmission Specification』などを参照している。本書は、PIVカードを併用する他のバイオメトリック方式の使用を妨げるものではない。

1 個人向けに発行される物理的な制作物（たとえば、ID カードや「スマート」カードなど）であり、カード所有者が主張する識別情報を、格納されている証明情報と照合して別の人物が検証したり（人間による読み取りおよび検証が可能な場合）、自動化されたプロセスによって検証したり（コンピュータによる読み取りおよび検証が可能な場合）できるように、身元証明情報（たとえば、写真、暗号鍵、バイオメトリックデータなど）が格納されているもの。

目次

1. はじめに 1
1.1 作成機関 1
1.2 目的および有効範囲 1
1.3 対象読者、前提条件、および概要 1
2. 用語、略語、表記表 2
2.1 用語 2
2.2 略語 2
3. 指紋登録 3
3.1 適用範囲 3
3.2 指紋データの保持 4
3.3 指紋画像の取得 4
3.4 指紋テンプレートの仕様 5
3.4.1 原画像 5
3.4.2 カードの発行 6
3.4.3 特徴点レコード 6
3.5 政府機関によって保持される指紋画像フォーマット 9
3.6 身元調査用の指紋画像仕様 11
4. 指紋認証センサーの仕様 12
4.1 適用範囲 12
4.2 PIV認証指紋の取得に関する仕様 12
5. 顔画像の仕様 13
5.1 適用範囲 13
5.2 取得とフォーマット 13
6. PIVバイオメトリックデータの共通ヘッダ 16
7. 性能試験および認証手続き 19
7.1 適用範囲 19
7.2 PIV認証 19
7.3 試験の概要 19
7.3.1 テンプレート生成プログラム 20
7.3.2 テンプレート照合プログラム 22
7.4 試験手順 22
7.5 相互運用可能グループの決定 23
7.6 PIVにおけるバイオメトリックシステムのパフォーマンス 23
8. 本仕様へのコンフォーマンス 25
8.1 コンフォーマンス 25
8.2 PIV登録指紋取得仕様へのコンフォーマンス 25
8.3 PIVカード指紋テンプレートレコードへのコンフォーマンス 25
8.4 政府機関が保持するPIV登録指紋のコンフォーマンス 25
8.5 PIV身元調査レコードのコンフォーマンス 25
8.6 PIV認証指紋取得仕様へのコンフォーマンス 25
8.7 PIV顔画像レコードのコンフォーマンス 25
8.8 CBEFF格納のコンフォーマンス 26
8.9 テンプレート生成プログラムのコンフォーマンス 26
8.10 テンプレート照合プログラムのコンフォーマンス 26
9. 参考文献 27

図のリスト

図 1 : PIV指紋画像のフロー 3
図 2 : 特徴点の角度の決定 8

表のリスト

表 1: 指紋取得プロトコル 4
表 2: フルセットの指紋画像を取得するための品質管理手順 5
表 3: PIVカードテンプレート用INCITS 378 プロファイル 6
表 4: 政府機関による指紋画像の保持のためのINCITS 381 プロファイル 9
表 5: 身元調査用レコードタイプ 12
表 6: PIV顔画像のINCITS 385 プロファイル 13
表 7: 簡略化したCBEFFの構造 16
表 8: パトロンフォーマットPIV仕様 16
表 9: CBEFFバイオメトリックデータタイプのコード化 18
表 10: INCITS 381 PIVカードテンプレート生成プログラム認証への入力仕様 20
表 11: INCITS 378 PIVカードテンプレート生成プログラムおよびPIVテンプレート照合プログラムの認証仕様 21

1. はじめに

1.1 作成機関

この文書は、NIST が、2002 年の連邦情報セキュリティマネジメント法（FISMA: Federal Information Security Management Act）、公法 107-347 に基づき、その法的責任を推進するために作成したものである。

NIST は、すべての連邦機関の運営および資産に適切な情報セキュリティをもたらすために、最低要件を含んだ標準および指針を作成する責任があるが、このような標準およびガイドラインは国家的セキュリティシステムには適用されない。この勧告は、行政管理予算局（OMB: Office of Management and Budget）Circular A-130、第 8b(3)項、『政府機関の情報システムの保護（Securing Agency Information Systems）』の要件と一致しており、これは A-130 の付録 IV「重要部門の分析」で分析されているとおりである。補足情報は、A-130、付録 III に記載されている。

この勧告は連邦諸機関が使用する目的で作成されている。この勧告は、非政府組織も自由意志で使用することができる。著作権による制約も受けない(翻訳者注:著作権に関するこの記述は、SP800-76 の英語の原文のことを言っており、日本語へ翻訳した本書の著作権は、独立行政法人 情報処理推進機構 及び NRI セキュアテクノロジーズ株式会社に帰属する)。本文書における一切は、商務長官が法的権威に基づき連邦政府に対して義務および拘束力を与えた標準およびガイドラインを否定するものではない。また、この勧告は、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威に変更を加えたり、これらに取って代わるものと解釈してはならない。

1.2 目的および有効範囲

FIPS 201『Personal Identity Verification (PIV) for Federal Employees and Contractors』[FIPS]は、識別情報の検証、登録、PIV カードの発行、PIV カードの利用など、PIV ライフサイクル活動に関する手順を定義している。FIPS はまた、バイオメトリックデータなどの身元証明情報の構造も定義する。バイオメトリックデータの暗号保護に関する要件は、[FIPS]および[800-78]にも記載されている。

本書は、[FIPS]の中で要求されているバイオメトリックデータの技術仕様を含む。これらの仕様は、PIV カードの相互運用性と性能上の設計目標を反映したものである。この仕様は、身元調査、指紋テンプレートの作成、保管、および認証を支援するための画像の取得を扱う。バイオメトリック標準を規範的に引用し、標準に選択肢や分岐がある要件を列挙することにより、目標に対応する。その場合、バイオメトリックプロファイルを用いて必須項目と任意選択項目を対比して明らかにすることができる。本書では、標準を実装者が解釈する際の制約をさらに強めている。かかる制約は、PIV アプリケーションに適した方法で実装を容易にし、コンフォーマンスを確保し、相互運用性を促進し、性能を保証するために策定したものである。

本書が取り扱うバイオメトリックデータの仕様は、PIV データモデル(SP 800-73-1 の付録 A を参照)におけるバイオメトリックデータにとって必須のフォーマットである。PIV データモデル以外でのみ使用されるバイオメトリックデータに関しては、本規格の範囲外である。

しかし本書では、PIV データモデルにおけるすべてのバイオメトリックデータが、第 6 節の CBEFF（Common Biometric Exchange Formats Framework）構造に格納されることを規定している。本書には、標準へのコンフォーマンスを試験する方策の概要が記述されている。ただし、それらは本書で規定する仕様に準拠することの認証や実証に用いることができる、包括的な一連の試験要件となるものではない。

1.3 対象読者、前提条件、および概要

本書は、連邦政府機関および PIV システムの実装者を対象としている。読者に、バイオメトリック標準および応用に関する実用上の知識があることを前提としている。本書の第 3 節で、指紋取得プロセス、PIV カードの特徴点テンプレートのフォーマット、および政府機関が任意に行う画像保持の保存フォーマットを定義する。第 4 節では指紋を媒体とする照合の実装に対する要件を述べ、第 5 節では顔画像の取得と保存用のフォーマットを規定する。第 6 節では、すべての PIV バイオメトリックデータの一般的なヘッダを定める。第 7 節と第 8 節は、それぞれ認証とコンフォーマンス試験を扱う。最後に、第 9 節は参考文献の一覧である。

2. 用語、略語、表記表

2.1 用語

用語	定義
セグメンテーション	指紋の場合、セグメンテーションとは 1 枚の N 指の画像を N 枚の単指の画像に分けることである。

2.2 略語

略語	定義
ANSI	American National Standards Institute（米国規格協会）
CBEFF	Common Biometric Exchange Formats Framework（共通バイオメトリック交換フォーマットフレームワーク）
FIPS	Federal Information Processing Standard（連邦情報処理規格）
EFTS / F	Electronic Fingerprint Transmission Specification (Appendix F)（電子指紋送信仕様（付録 F）
INCITS	InterNational Committee for Information Technology Standards（情報技術規格国際委員会）
ISO	International Organization for Standardization （国際標準化機構）
IEC	International Electrotechnical Commission（国際電気標準会議）
NFIQ	NIST Fingerprint Image Quality（NIST 指紋画像画質）
NIST	National Institute of Standards and Technology（米国国立標準技術研究所）
PIV	Personal Identity Verification（個人識別情報の検証）
WSQ	Wavelet Scalar Quantization（ウェーブレットスカラー量子化）

3. 指紋登録

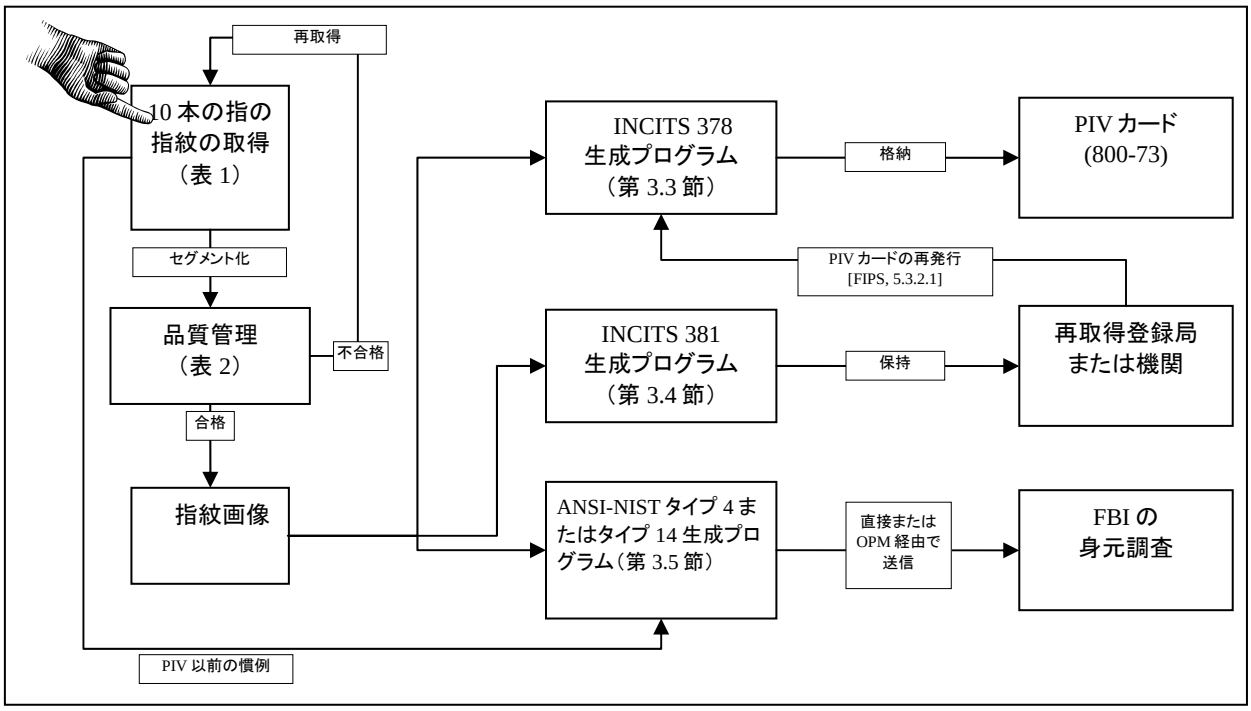
3.1 適用範囲

この節の仕様は、必須の PIV バイオメトリック登録データの作成に関連する。つまり、この節では指紋画像とテンプレートの取得、フォーマット設定、および格納について説明する。この節で説明する資料の概要を以下に示す。

+ 第 3.2 節では、指紋画像を取り込んで PIV に登録するための指紋スキャナの使用法についての仕様を説明する。
+ 第 3.4 節では、PIV カードに格納する指紋テンプレートのフォーマットについて説明する。
+ 第 3.5 節では、政府機関が保持する指紋画像の仕様について説明する。
+ 第 3.6 節では、身元調査用に FBI に送信するのに適したレコードへの指紋の変換を規定する。

FBI の要件によってセンサーの仕様も推進されるが、第 3.4 節と第 3.5 節で規定される永続的な電子格納フォーマットは、INCITS（つまり FBI 以外）規格のレコードであるため、別個に規定される点に注意のこと。図 1 に指紋の取得と格納の手順を示す。

図 1 : PIV 指紋画像のフロー



3.2 指紋データの保持

本書は、政府機関に対して指紋画像を保持することを求めるものでもなければ、そのような活動を禁止するものでもない。しかしながら、画像を保持しようとするのであれば、第 3.5 節に記載のフォーマットに従って保存する必要がある。このフォーマットには、第 6 節に記載の CBEFF ヘッダが含まれていて、画像レコードを暗号化できるようになっている。

本書は、政府機関に対して指紋のテンプレートを保持することを求めるものでもなければ、そのような活動を禁止するものでもない。しかしながら、テンプレートを政府機関固有のフォーマットや標準フォーマットで保持しようとするのであれば、それらのテンプレートを第 6 節に記載の CBEFF ヘッダに含める必要がある。これによりレコードを暗号化できる。

データの保持は、重複する識別情報の検知などを支援する。

3.3 指紋画像の取得

この節では、PIV に登録するためのフルセットの指紋画像の取り込みについて規定する。対象者の指紋は、表 1 に示す 3 つの画像モードのいずれかに従って集めなければならない。

表1: 指紋取得プロトコル

<table>
<tr><th colspan="2">オプション 1 – 平面指紋のライブスキャンに必要な表現</th></tr>
<tr><td colspan="2">右手の 4 本の指（親指以外）を組み合わせた平面指紋の押捺</td></tr>
<tr><td colspan="2">左手の 4 本の指（親指以外）を組み合わせた平面指紋の押捺</td></tr>
<tr><td colspan="2">2 本の親指を組み合わせた指紋の押捺</td></tr>
<tr><th colspan="2">オプション 2 – 回転指紋のライブスキャンに必要な表現</th></tr>
<tr><td colspan="2">10 本の指の個別回転指紋</td></tr>
<tr><td colspan="2">右手の 4 本の指（親指以外）を組み合わせた平面指紋の押捺</td></tr>
<tr><td colspan="2">左手の 4 本の指（親指以外）を組み合わせた平面指紋の押捺</td></tr>
<tr><td>左手親指の平面指紋の押捺</td><td rowspan="2">これらの取り込みは、同時(2つの親指を隣り合わせにして置く)または順次(1 回につきどちらか片方の親指だけを置く)に行える。</td></tr>
<tr><td>右手親指の平面指紋の押捺</td></tr>
<tr><th colspan="2">オプション 3 – カードへの回転指紋の転写に必要な表現</th></tr>
<tr><td colspan="2">10 本の指の個別回転指紋</td></tr>
<tr><td colspan="2">右手の 4 本の指（親指以外）を組み合わせた平面指紋の押捺</td></tr>
<tr><td colspan="2">左手の 4 本の指（親指以外）を組み合わせた平面指紋の押捺</td></tr>
<tr><td>左手親指の平面指紋の押捺</td><td rowspan="2">これらの取り込みは、同時(2つの親指を隣り合わせにして置く)または順次(1 回につきどちらか片方の親指だけを置く)に行える。</td></tr>
<tr><td>右手親指の平面指紋の押捺</td></tr>
</table>

参考情報:

1. 画像を取得するための順序は、上記の順序である必要はない。
2. 複数の指を組み合わせた平面指紋の押捺画像は、スラップまたはフラットとも呼ばれる。特定の回転動作を行わずに、複数の指を同時に画像処理表面に置くことによって画像を取得する。
3. オプション 2 と 3 は、政府機関の現行の慣例を表す。最近では、オプション 1 が FBI に受け入れられているが、OPM(人事局)を介したデータ転送では、オプション 2 または 3 の実施が必要となる場合もある。

オプション 1 と 2 では、指紋の取り込みに使用する装置が FBI の電子指紋送信仕様の付録 F[EFTS、付録 F]に準拠していることを FBI が認証しなければならない。オプション 3 では、電子フォームに変換するために、転写されたカードのスキャンが実行される。スキャナは、FBI によって[EFTS、付録 F]に準拠したものであることが認証されなければならない。第 3.5 節と第 3.6 節で説明している電子フォーマットの指紋を生成するにはスキャンが必要である。FBI 仕様には、画像処理表面の幅と高さの仕様が含まれている。この装置のネイティブのスキャン解像度は、水平方向と垂直方向のいずれも 1 センチ当たり 197 ピクセル（1 インチ当たり 500 ピクセル）でなければならない。これらの仕様は、FBI の提出要

件、および指紋画像ベースのデータ交換フォーマット標準の画像取得設定レベル 31（INCITS 381、[FINGSTD]）に準拠している。

指紋の収集は、表 2 に示す手順に従わなければならない。手順は、必要な画像の再取得を開始するための NIST 指紋画像画質[NFIQ]アルゴリズムを採用しなければならない。指紋の取得時には、立会い責任者が同席しなければならない。指紋を取得する際には、立会い責任者が同席しなければならない。政府機関は、画像取得の品質を保証し、意図的であるなしにかかわらず誤った提示がなされるのを防ぐための、対策を講じるべきである。このような活動は、画像取り込み装置の総合的な機能によって実施される場合もあれば、立会い責任者によって実施される場合もある。どのようなケースであっても責任者は、申請者が指の位置や手を入れ替えたり、指をさえぎったり、ずらしたり、誤った位置に置いたりしないことを確認する。特に、複数指の平面指紋の押捺では、第 5 指と第 10 指が短いために画像取得用プラテンに届かないことが多いので、平面に対してある角度をなすように手を置くことで、4 本の指がすべて画像に収まるようにすることが慣例となっている。最新の大型プラテンを備えているデバイスでは、このような慣行を必要としないが、立会い責任者はあらゆるケースにおいてすべての対象指が完全に画像に収まるように、注意を払わなければならない。この手順では、複数指の平面指紋の押捺をセグメント化する必要があるが、この操作は立会い責任者が支援できる。

表2: フルセットの指紋画像を取得するための品質管理手順

ステップ	アクション
1.	立会い責任者は、指紋を検査し、異物をなくすように要求しなければならない。
2.	責任者は、センサーの画像処理表面、つまりカードが汚れていないことを確認しなければならない。
3.	表 1 のオプション 1、2、または 3 に従って指紋を取得する。オプション 3 については、[EFTS、付録 F]で認証されたスキャナを使用して転写されたカードをスキャンする。
4.	複数指の平面指紋の押捺画像を、単指の画像にセグメント化する。自動セグメント化を推奨する。立会い責任者は自動セグメント化の境界を検査し、インタラクティブなグラフィカルユーザインタフェースなどによって全ての障害を是正する。
5.	親指と人差し指の NFIQ 値を計算する。すべての NFIQ 値が 1、2、または 3（つまり画質がよい）であれば、ステップ 8 に進む。
6.	あと 3 回まで、ステップ 2～5 を繰り返す。
7.	4 回取得した結果、人差し指と親指の NFIQ 値が 1、2、または 3 ばかりではない場合は、ステップ 3 で取得されてステップ 4 でセグメント化され、左手人差し指、右手人差し指、左手親指、右手親指の NFIQ 値の平均が最小であるセット（つまり最良の画質）を選択する。人差し指と親指の画質値のすべてが使用できるとは限らない場合は（おそらく、1 本または複数の指をけがしているなどの理由で）、ステップ 3 で取得した取得可能な指の最後のセットを、NFIQ を一切適用しないで使用する。
8.	第 3.4 節、第 3.5 節、および第 3.6 節に従って、最終レコードを準備して格納する。

通常、このプロセスでは 10 本すべての指の指紋画像を取るが、1 本または複数の指が取れない場合（たとえば切断などの理由）、取れるだけの指の画像を取得する。収集した画像が 10 本未満である場合、第 3.4 節の FBI のバックグラウンドトランザクション（添付されるタイプ 2 レコードの AMP 2.084 フィールド）によって、切断されたかその他の理由で画像を取得できない指のラベル付けが必要である。[EFTS、付録 C]を参照のこと。

3.4 指紋テンプレートの仕様

この節では、[FIPS]が指定する PIV の必須バイオメトリック要素の生成方法と格納方法を規定する。この仕様は、PIV カード内に格納されるテンプレート、および[MINUSTD]テンプレートに適用（そうでない場合は政府機関によって保持される）される。このテンプレートは、PIV 認証のための登録バイオメトリックから構成されるので、高画質取得のための仕様および FBI が認証する圧縮フォーマットによってサポートされる。この節の標準化されたテンプレート仕様によって、複数ベンダー製品環境で PIV カードが使用できる。

3.4.1 原画像

2 つの[MINUSTD]指紋テンプレートが PIV カードに格納される。これ以降、これらを PIV カードテンプレートと呼ぶ。これらは、第 1 指と第 2 指の画像から準備される（[FIPS]で仕様が定められているとおり）。これらの画像は、PIV 登録時に取り込まれたフルセットの平面指紋の押捺をセグメント化して取得されたもので、表 2 の 8 行目に格納される。

激しいローテーションを伴う複数指の平面指紋の押捺（例えば、狭小のプラテンを使用して、4 本の指の画像を取得する場合）は、必須特徴点テンプレートを生成する前に、または生成プロセスの一環として除去しなければならない。回転角は、指関節のしわがほぼ水平になるようにするか、それと等価であるが、それぞれの指の隙間がほぼ垂直になるようにする。この要件を満たすことによって、相互運用が可能な指紋照合を実現できる。

3.4.2 カードの発行

PIV カードの発行時に、[FIPS, 5.3.1]に従って 1 つまたは複数の認証を試行しなければならない。このために、第 1 指と第 2 指両方の指紋を新たにライブで取り込み、PIV カードテンプレートと照合する必要が生じる。これでカード保持者が、身元が確認された個人と結び付けられる。この認証では、第 3.2 節に記載の複数指の指紋画像取り込み装置である[EFTS/F]、または第 4 節に記載の[SINGFING]装置を使用して収集した画像を使用する。

3.4.3 特徴点レコード

PIV カードテンプレートは、INCITS 378-2004 [MINUSTD]特徴点テンプレート標準の適合例でなければならない。つまり、第 1 指と第 2 指の両方の特徴点が 1 つの INCITS 378 レコード内に存在しなければならない。これは、一般レコードヘッダ[MINUSTD, 6.4]の 1 つのインスタンスと、フィンガービューレコード[MINUSTD, 6.5]の 2 つのインスタンスが存在することを意味する。PIV カードに格納する前に、このレコードを第 6 節で説明する CBEFF 構造を持つ単一インスタンスに格納しなければならない。PIV カードテンプレートは、暗号化してはならない。

表 3 は、一般的な[MINUSTD]標準のプロファイルである。この仕様は、PIV カードに格納されるすべての特徴点テンプレートに適用しなければならない。非常に正確で相互運用可能な個人識別情報の検証を促進するために、これらの制約が含まれている。本文書では、画像を取り込んでから格納用に圧縮するまでの間に、特徴点レコードを準備することを推奨する（図 1 を参照）。

INCITS 378 は、INCITS M1 委員会によって改訂されると考えられる。これらの改訂内容は、PIV と直接関係のあるものではない。 しかしながら、実装については表 3 の 14 行目のバージョン番号の規定に従わなければならない。

実装者を支援するために、NISTでは[MINUSTD]のサンプルデータ [2]を提供している。

表3: PIV カードテンプレート用 INCITS 378 プロファイル

			節の表題および／またはフィールド名（かっこ内の番号は[MINUSTD]の章番号）	INCITS 378-2004		PIV コンフォーマンス	備考
				フィールドまたは内容	必須値	許容値	
1.			原則(5.1)	NC		A	指紋の特徴点を定義する。
2.			特徴点のタイプ (5.2)			注 1 を参照	[MINUSTD, 5.2]では特徴点のタイプを定義するが、規定の内容は含まない。
3.			特徴点の位置：座標系(5.3.1)	NC		A	特徴点の位置の計算に使用する定義。
4.			特徴点の位置：端点での特徴点の配置(5.3.2)	NC		A	
5.			特徴点の位置：分岐点での特徴点の配置(5.3.3)	NC		A	
6.			特徴点の位置：他の特徴点のタイプでの特徴点の配置(5.3.4)	NC		注 1 を参照	
7.			特徴点の方向：角度の規則(5.4.1)	NC		A	特徴点の角度の計算に使用する定義。
8.			特徴点の方向：端点の角度(5.4.2)	NC		A	

[2] PIV 規格に適合する特徴点レコードは、http://www.itl.nist.gov/iad/894.03/nigos/piv_sample_data.html を参照のこと。これらのレコードは、http://www.itl.nist.gov/iad/894.03/nigos/incits.html から入手可能な NIST のソフトウェアを使用して作成されたものである。

			節の表題および／またはフィールド名（かっこ内の番号は[MINUSTD]の章番号）	INCITS 378-2004		PIV コンフォーマンス	備考
				フィールドまたは内容	必須値	許容値	
9.			特徴点の方向：分岐点の角度(5.4.3)	NC		A	
10.	一般レコードヘッダ		バイト順(6.2)	NC		A	ビッグエンディアン、符号なし整数
11.			特徴点レコードの編成(6.3)	NC		A	
12.			CBEFF レコードのヘッダ(6.4)	MF	MV	パトロンフォーマット PIV	複数フィールド CBEFF ヘッダ、第 6 節
13.			フォーマット ID (6.4.1)	MF	MV	0x464D5200	ASCII "FMR¥0"
14.			バージョン番号(6.4.2)	MF	MV	0x20323000	ASCII "020¥0"（INCITS 378-2004）。注 2 を参照。
15.			レコード長(6.4.3)	MF	MV	26 ≤ L ≤ 1574	これは 2 バイトフィールドを意味する。注 3 を参照。
16.			CBEFF 製品 ID の所有者(6.4.4)	MF	MV	> 0	注 4 を参照。
17.			CBEFF 製品 ID のタイプ (6.4.4)	MF	MV	> 0	注 4 を参照。
18.			取り込み装置の適合(6.4.5)	MF	MV	1000b	センサーは、PIV 登録要件に従って EFTS 付録 F に適合。
19.			取り込み装置 ID (6.4.6)	MF	MV	> 0	注 5 を参照。
20.			スキャン画像の x 方向のサイズ (6.4.7)	MF	MV	MIT	注 11 を参照。
21.			スキャン画像の y 方向のサイズ (6.4.8)	MF	MV	MIT	
22.			X（水平）方向の解像度(6.4.9)	MF	MV	197	親画像は第 3.4.1節に適合。
23.			Y（垂直）方向の解像度(6.4.10)	MF	MV	197	
24.			指表示の数(6.4.11)	MF	MV	2	第 1 指と第 2 指それぞれに 1 回ずつ
25.			予約バイト (6.4.12)	MF	MV	0	
26.	指表示レコード（K インスタンス分）	表示ヘッダ	指表示のヘッダ (6.5.1)	NC		A	
27.			指の位置(6.5.1.1)	MF	MV	MIT	
28.			表示番号(6.5.1.2)	MF	MV	0	注 10 を参照。
29.			押捺タイプ (6.5.1.3)	MF	MV	0 または 2	ライブスキャンまたはライブスキャン以外の平面指紋の画像。
30.			指の画質(6.5.1.4)	MF	MV	20,40,60,80,100	注 6 を参照。
31.			特徴点の数(6.5.1.5)	MF	MV	0 ≤ M ≤ 128	M 個の特徴点データレコードが続く。
32.		指紋特徴点データ（M インスタンス分）	特徴点タイプ (6.5.2.1)	MF	MV	01b, 10b, または 00b	注 1 を参照。
33.			特徴点の位置(6.5.2.2)	MF	MV	MIT	注 7 を参照。
34.			特徴点の角度(6.5.2.3)	MF	MV	MIT	注 8 を参照。
35.			特徴点の画質(6.5.2.4)	MF	MV	MIT	
36.			拡張データのブロック長(6.6.1.1)	MF	MV	0	注 9 を参照。
表の終り							

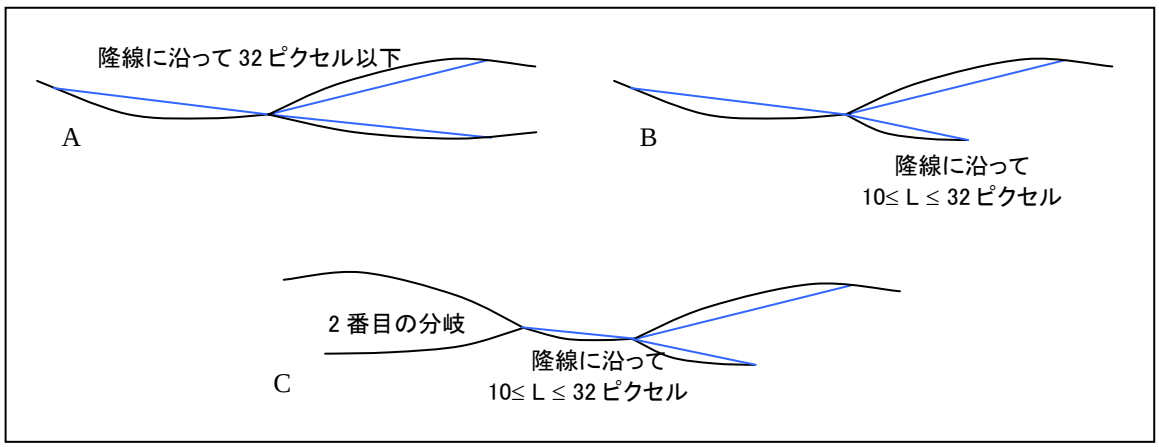
略語		意味
MF	必須フィールド	[MINUSTD] では、FMR にフィールドがなければならない。
MV	必須値	[MINUSTD] では、フィールドに意味のある値がなければならない。
NC	規定の内容	[MINUSTD] は、PIV の規定の慣例を示す。かかる節では、FMR 内にフィールドを定義しない。
A	必要に応じて	PIV の場合、値または慣例は[MINUSTD]の規定と同様である。
MIT	インスタンス化時に必須	PIV の場合、レコードのインスタンス化時に決定される必須値。[MINUSTD]で規定されている慣例に従う。

規定についての注意:

1. [MINUSTD]では、格納された各特徴点に、関連付けられたタイプが必要である。PIV の場合、必須のカードテンプレートは端点タイプまたは分岐点タイプの特徴点を含まなければならない。これらのタイプは、[MINUSTD, 5.3. {2,3}]で定義される。三分岐や交差など、ほかのタイプの特徴点が PIV カードテンプレートに含まれてはならない。ただし、端点と分岐点を確実に区別できない特徴点の場合、「ほか」のカテゴリはビット値 00b を使用して割り当ておよびコード化しなければならない。「ほか」のタイプの特徴点の角度と位置は、その特徴点がどちらでありそうかというコード化アルゴリズムの判断に応じて、対応する端点または分岐点に適用されたと考えられる角度と位置でなければならない。これは、画像転写が過大または過少なために、分岐点が端点に変換されたり端点が分岐点に変換されたりして見える「転写」押捺の一般的な特性である。
2. [MINUSTD, 6.4.2]の 2 番目のパラグラフは、ASCII スペースと、最初のパラグラフで言及している「3 つの ASCII 数字」の両方で構成される。バージョンナンバーの最初の文字として ASCII スペースを用いる場合は、次のような形式に従うものとする: "20\0" (すなわち、"0x20323000")。
3. レコード全体の長さは[800-73]が規定するコンテナーサイズの制限内に収まらなければならない。これらの制限は、[FACESTD]レコードだけでなく、CBEFF で格納された署名済みエンティティ全体に適用される。
4. [MINUSTD, Section 6.4.4]の CBEFF 製品 ID の 2 つのフィールド("Owner"と"Type")は、両方ともゼロ以外でなければならない。最上位の 2 バイトでベンダーを識別し、最下位の 2 バイトでそのベンダーの特徴点検知アルゴリズムのバージョン番号を識別する。
5. 取り込み装置 ID が報告されなければならない。この ID を使用することによって、相互運用性が向上する。
6. 画質値は、[NFIQ]を使用して親画像について計算し、ここで Q = 20*(6 - NFIQ)として報告される値である。
7. 元の指紋画像については、特徴点のすべての座標と角度を記録しなければならない。テンプレートの作成プロセスで作成されるサブ画像の処理については、記録してはならない。
8. 特徴点の方向の判断は、各スケルトン分岐から引き出せる。すべてのスケルトン分岐の 3 本の線を調べて、それぞれの終点を決定しなければならない。図 2 の A から C に、線の終点を決定するための 3 つの方法を示す。終点は、以下に示す最初に発生した事象に従って確立される。
    - 32 番目のピクセル – 図 2 の A と B を参照 ー または
    - 10 ピクセルを超える場合はスケルトン線の終点(それより短い線は使用しない)– 図 2 の B を参照 ー または
    - 2 番目の分岐が 32 番目のピクセルの手前にある – 図 2 の C を参照。

特徴点の角度は、分岐点を起点としそれぞれの線の終点に伸びる 3 本の仮想放射線を描いて決める。放射線が形成する 3 つの角度の中で最も小さい角度を二等分して、特徴点の方向を示す。

図 2 : 特徴点の角度の決定



9. 必須値がゼロの場合、PIV カードテンプレートに拡張データを含めてはならないことが仕様で定められている。

10. [MINUSTD, 6.5.1.2]に従い、「表示番号」フィールドの値は、第 1 指と第 2 指ともに 0 でなければならない。「表示番号」フィールドの値と「指の位置」フィールドの値の組み合わせによって、それぞれのテンプレートを一意に識別することができる。

11. [MINUSTD]では、レコードの中に 2 つ以上のビュー(view)が含まれていて、それらのビューがサイズの異なる複数の画像から抽出されたものである場合には、ヘッダの中で画像サイズがどのように記録されるかについては規定しない。PIV では、表 3 の 20 行目の幅は、入力された 2 つの画像の幅のうちの大きい方の値でなければならない。同様に、21 行目の高さについても、入力された 2 つの画像の高さのうちの大きい方の値でなければならない。

3.5 政府機関によって保持される指紋画像フォーマット

この節では、第 3.2 節で収集した指紋画像を保持するための共通データフォーマットのレコードを規定する。特に、登録、その他の方法で政府機関が保持する指紋画像は、INCITS 381-2004 の指紋画像に基づくデータ交換フォーマット標準[FINGSTD]に従ってフォーマットしなければならない。このセットは、10 枚の単指画像を含まなければならない。これらの画像は、表 1 のオプション 1、2 または 3 に従って集められた複数指の平面指紋画像のセグメント化、およびオプション 2 と 3 の表現 4 と 5 からの 1 本の親指の平面指紋の押捺から取得される。これらの画像は、1 つの[FINGSTD]レコードに格納される。このレコードは、関連付けられた複数指の平面指紋の押捺と回転指紋の画像を含むこともある。この文書（[800-76]）では、表 1 のオプション 2 または 3 に従って集められた単指の回転指紋の画像の使用については規定しない。レコードは、第 6 節で説明する CBEFF 構造で格納しなければならない。政府機関は、第 6 節の表 9 の注 2 の規定に従って、このデータを暗号化できる。

表 4 に、[FINGSTD]の章ごとのプロファイルを示す。この表の第一の目的は、オプションの内容を持つ[FINGSTD]のフィールドに対して PIV 仕様を示すことである。1～10 行は規定の内容である。11 行目は、第 6 節で説明する CBEFF 構造を必要とする。ただし、その FASC-N 値（表 8 の 13 行目）は、次のような場合に例外として、すべてがゼロのフィールドによって置き換えられることがある：FASC-N が割り当てられる前に、PIV の登録画像が保存される。このようなインスタンス(電子署名を含む)は、FASC-N が確定した後で、再度生成する必要がある。12～27 行は、[FINGSTD、表 2]の一般レコードヘッダのフィールドに対して PIV 仕様を示す。これらは、レコードのすべての画像に共通である。同様に、28～36 行に[FINGSTD]表 4 の指紋画像ヘッダレコードの仕様を示す。"PIV Conformance"の列は、PIV 固有の慣例および標準のパラメータのデフォルトを示す。

INCITS381 は、INCITS M1 委員会によって改訂されると考えられる。これらの改訂内容は、PIV と直接関係のあるものではない。しかしながら、実装については表 4 の 14 行目のバージョン番号の規定に従わなければならない。

実装者を支援するために、NISTでは[FINGSTD]のサンプルデータ[3]を提供している。

表4: 政府機関による指紋画像の保持のための INCITS 381 プロファイル

			節の表題および／またはフィールド名（かっこ内の番号は[FINGSTD]の章番号）	INCITS 381-2004		PIV コンフォーマンス	備考
				フィールドまたは内容	必須値	許容値	
1.			バイトおよびビットの順序(5.1)	NC		A	ビッグエンディアン、最上位ビット－最下位ビットの順
2.			スキャン順序(5.2)	NC		A	
3.			画像取得要求 (6)	NC		レベル 31	表 1
4.			ピクセル縦横比(6.1)	NC		A	1:1

3 規格に適合する手指指紋の画像は、http://www.itl.nist.gov/iad/894.03/nigos/piv_sample_data.html を参照のこと。これらの画像は、http://www.itl.nist.gov/iad/894.03/nigos/piv_sample_data.html から入手可能な NIST のソフトウェアを使用して作成されたものである。

			節の表題および／またはフィールド名（かっこ内の番号は[FINGSTD]の章番号）	INCITS 381-2004		PIV コンフォーマンス	備考
				フィールドまたは内容	必須値	許容値	
5.			ピクセルデプス(6.2)	NC		A	レベル 31 → 8
6.			グレースケールデータ(6.3)	NC		A	レベル 31 →ピクセル当たり 1 バイト
7.			ダイナミックレンジ (6.4)	NC		A	レベル 31 → 200 グレーレベル
8.			スキャン解像度(6.5)	NC		A	レベル 31 → 500 ppi
9.			画像解像度(6.6)	NC		197	1 センチ当りのピクセル数 – 補間なし
10.			指紋画像の位置(6.7)	NC		A	スラップ配置情報、中央揃え
11.			CBEFF ヘッダ (7)	MF	MV	パトロンフォーマット PIV	複数フィールド CBEFF ヘッダ、第 6 節
12.			一般レコードのヘッダ (7.1)	NC		A	
13.	指紋画像レコードフォーマット		フォーマット ID (7.1.1)	MF	MV	0x46495200	ASCII ″FIR¥0″
14.			バージョン番号(7.1.2)	MF	MV	0x30313000	ASCII ″010¥0″
15.			レコード長(7.1.3)	MF	MV	MIT	CBEFF 構造を除いたサイズ
16.			CBEFF 製品 ID の所有者(7.1.4)	MF	MV	＞0	CBEFF PID.
17.			CBEFF 製品 ID のタイプ(7.1.4)	MF	MV	＞0	
18.			取り込み装置 ID (7.1.5)	MF	MV	MIT	指定されたベンダー。注 1 を参照。
19.			画像取得レベル (7.1.6)	MF	MV	31	設定レベル 31
20.			画像数(7.1.7)	MF	MV	MIT	K で示す。28～37 行を参照のこと。注 2、3 および 4 を参照のこと。
21.			尺度の単位(7.1.8)	MF	MV	0x02	センチメートル
22.			スキャン解像度（水平）(7.1.9)	MF	MV	197	1 センチ当たりのピクセル数
23.			スキャン解像度（垂直）(7.1.10)	MF	MV	197	
24.			画像解像度（水平）(7.1.11)	MF	MV	197	
25.			画像解像度（垂直）(7.1.12)	MF	MV	197	
26.			ピクセルデプス (7.1.13)	MF	MV	8	256 階調のグレースケール
27.			画像圧縮アルゴリズム (7.1.14)	MF	MV	0 または 2	非圧縮または WSQ。注 5 および 6 を参照。
28.			予備(7.1.15)	MF	MV	0	2 バイト、注 12 を参照。
29.	指紋（K 個）または複数指紋		指紋データのブロック長(7.2.1)	MF	MV	MIT	
30.			指の位置(7.2.2)	MF	MV	MIT	
31.			表示の数(7.2.3)	MF	MV	≥ 1	この指の M 個の表示。注 7 を参照。
32.		指紋表示（M 個）	表示番号(7.2.4)	MF	MV	MIT	
33.			指紋画像の画質(7.2.5)	MF	MV	20,40,60,80,100	変換された NFIQ。注 8 および 9 を参照。
34.			押捺タイプ (7.2.6)	MF	MV	0 または 2	ANSI NIST ITL 1-2000 を参照。
35.			水平線の長さ (7.2.7)	MF	MV	MIT	注 10 を参照。
36.			垂直線の長さ (7.2.8)	MF	MV	MIT	
37.			予備(章なし)	MF	MV	0	注 11 を参照。
38.			指紋画像データ(7.2.9)	MF	MV	MIT	非圧縮または WSQ 圧縮データ
表の終り							

略語		意味
MF	必須フィールド	[FINGSTD] は、レコードにフィールドが存在することを要求する。
MV	必須値	[FINGSTD] は、このフィールドに意味のある値を要求する。
NC	規定の内容	[FINGSTD] は、PIV の規定の慣例を示す。かかる節では、FIR 内にフィールドを定義しない。
A	標準の要求に応じて	PIV の場合、値または慣例は[FINGSTD]の規定と同様である。
MIT	インスタンス化時に必須	PIV の場合、レコードのインスタンス化時に決定される必須値。[FINGSTD]に規定されている慣例に従う。

規定についての注意:

1. 取り込み装置 ID は、ハードウェアモデルを示さなければならない。CBEFF PID [FINGSTD, 7.1.4]は、ファームウェアまたはソフトウェアのバージョンを示さなければならない。
2. 特定の指の画像を取得できない場合は、このフィールドの値をその分減らさなければならない。
3. 左手と右手の 4 本の指の画像、および 2 本の親指の画像を含めることもできる。このフィールドの値を、その分増やさなければならない。
4. PIV 登録セットの場合、画像の数は通常 13 枚(つまり、複数指の平面指紋の押捺から得られた 10 枚のセグメント化画像、および 3 枚の平面指紋の押捺自体)、または 14 本(親指の平面指紋の押捺画像が別々に取得されたとき)である。
5. 画像は非圧縮にするか、または FBI によって認証された WSQ(Wavelet Scalar Quantization:ウェーブレット/スカラー量子化)アルゴリズムの実装を使用して圧縮しなければならない。15:1 という、FBI の現行の公称圧縮率の要件を適用しなければならない。
6. 圧縮を行うのは、第 3.4 節および第 3.6 節で要求されるレコードを用意し、変換された NFIQ 値を割り当てた後でなければならない。
7. 「表示」という用語は、特定の指の画像数を示す。画像処理を繰り返した場合は、この値が 1 を超えることがある。単指の画像を複数枚含めると、照合プロセスでいくつかの利点がもたらされる。本文書では、画質値 1〜3 を持つ画像がさらに利用できれば(たとえば、PIV カードの再発行手順で得られた画像)、レコードに含めることを推奨している。どの場合も、取り込み日が最新の画像が最初に置かれる順序で格納しなければならない。
8. 画質値を記入しなければならない。これらの値は、[NFIQ]で説明した NFIQ(NIST Fingerprint Image Quality:NIST 指紋画像画質)方式によって、Q = 20*(6 - NFIQ)という式を使用して計算しなければならない。この尺度の反転によって、高い画質値が高い予想性能を確実に意味し、辞書の定義との整合性が確保される。この値は、特徴点に基づく指紋照合システムの相対的な性能を予測するように意図されている。ユーザーが最初に認証しようとするときには、第 1 指または第 2 指のどちらでも、最高画質の指を使うことを推奨する。
9. このレコードが単指の指紋でない(つまり、複数指の画像または掌紋である)場合、または NFIQ の実装に失敗した場合、画質値を 254(未定義を示す[FINGSTD]コード)としなければならない。
10. 画像サイズには制限はない。ただし、対象とする指の背景部分以外のピクセルは維持しなければならない(つまり、画像データのトリミングは禁止されている)。
11. [FINGSTD、表 4]には、「予備」という 1 バイトのフィールドがあるが、このフィールドを正式に定義する章はない。M1 委員会では、この問題を解決するために、「予備」フィールドをレコードに含めることを求める新たな従属節の導入を提案した。この従属節は、[FINGSTD]の改訂版に記載される予定である。いかなる場合でも、PIV を導入する場合には、値を 0 に設定した 1 バイトの「予備」フィールドを含めなければならない。
12. 表の中の 27 行目は、「予備」フィールドの長さが 2 バイトでなければならないことを示している。[FINGSTD、7.1.15]では、この長さが 4 バイトであり、[FINGSTD、表 2]の値と一致しない。INCITS M1 委員会では、2 バイトが正しい値であるとしている。PIV を導入する場合には、値を 0 に設定した 2 バイト長の「予備」フィールドを含めなければならない。

3.6 身元調査用の指紋画像仕様

身元調査プロセスの一環としてFBIに送信される PIV 指紋画像は、ANSI/NIST-ITL 1-2000 標準[FFSMT]および CJIS-RS-0010 [EFTS]仕様に従ってフォーマットしなければならない。このようなレコードは、第 3.1 節の仕様に従って収集された画像の中のみから準備し、含めなければならない。

表 5 に、第 3.2 節の 3 つの取得オプションに対する適切なトランザクションフォーマットを列挙する。最終的な要件については、FBI 文書[EFTS]を参考にしなければならない。

表5: 身元調査用レコードタイプ

オプション	[FFSMT]参考資料での トランザクションデータのフォーマット	参考資料
1	3 個のタイプ 14 レコード（注 1 を参照）	[EFTS、付録 N]。注 2 を参照。
2 または 3	14 個のタイプ 4 レコード(注 1 を参照)	[EFTS]第 3.1.1.4 節「Federal Applicant User Fee」

規定についての注意:

1. FBI とのトランザクションでは、すべてのタイプでデータにタイプ 1 と 2 の両方のレコードを添付する必要がある。[FFSMT, 表 2]を参照のこと。タイプ 2 は、欠落している指のラベル付けに対応している。
2. 今後の[FFMST]の改定（2007 年初旬の予定）では、タイプ 14 レコードに新しいフィールドがいくつか追加される予定であるが、これは古いバージョンとの互換性が維持されるように実施される。しかしながら、どの場合でも、[EFTS,付録 N]は画像フォーマットの最終的な参考資料となる。

4. 指紋認証センサーの仕様

4.1 適用範囲

この節では、ライブ認証用（PIV カード所有者の認証用）の指紋を取り込むのに使用する、すべての指紋センサーの仕様を示す。この仕様は第 3.4 節で説明した必須の PIV カードテンプレートを使用する、すべてのセンサーに適用される。この仕様は第 3 節で説明した登録に関する仕様とは無関係である。

4.2 PIV 認証指紋の取得に関する仕様

PIV 認証に使用する指紋センサーは FBI の単指画像取り込み装置の画像品質仕様(Image Quality Specifications For Single Finger Capture Devices)である[SINGFING]に適合しなければならない。[SINGFING] 仕様では、このような装置の画像取得用プラテンとスキャン解像度の最小サイズを規定している。

5. 顔画像の仕様

5.1 適用範囲

[FIPS、第 4.4.1 節]では、PIV 申請者の顔画像の収集が必要で、この画像を印刷イメージの生成[FIPS、第 4.1.4.1 節]やカード保有者の本人認証の補強のためにも使用することを示している。本文書で示す顔仕様はこのような活動をサポートし、顔画像を保存するためのフォーマットを確立する。本書は、政府機関に対して顔画像を保持することを求めるものでもなければ、そのような活動を禁止するものでもない。しかしながら、顔画像を保持しようとするのであれば、本節に記載のフォーマットで保存する必要がある。他のバイオメトリック要素と同様、政府機関は PIV カードに顔データを保存して自動認証に使用することを選択してもよい。この節では、政府機関が任意に行う上記の活動に何らの規定要件も課さずに、バイオメトリック自動登録および顔認識に適した画像を規定する。

5.2 取得とフォーマット

この節では顔画像の保持に関する仕様を示す。PIV 登録時に収集された顔画像は、INCITS 385-2004 [FACESTD]に適合するフォーマットでなければならない。[FACESTD]は、フォーマットだけではなく顔画像の取得方法についても規定している。これは、画像品質の向上を通じて最終的に性能の向上を図るためである。画像は、第 6 節で定義する CBEFF 構造の中に組み込まれなければならない。[FACESTD]はアプリケーションをまたがる包括的な仕様なので、二者択一式の要件を含む節も含まれている。PIV 用に作成した[FACESTD]のアプリケーションプロファイルを表 6 に示す。これは、包括的な内容の多くを具体的な仕様として示している。第 3 列には該当する[FACESTD]の節を、第 4 列、5 列には[FACESTD]の要件を示す。表 6 の第 6 列は、PIV に対する規定の慣例または仕様値を示す。この表は実装コンフォーマンスステートメント（ICS）規格には適合していない。特に、この表では ICS 機能を拡張しているが、従来の ICS の構成に必要な行があるのでそのためにも役立つと考えられる。とはいえ、[ICS]の第 9.1 節に規定されている「サポートされる値の欄」が追加されており、実装者はこれを仕様へのコンフォーマンスのチェックのために使用しなければならない。

INCITS 385 は、INCITS M1 委員会によって改訂されることがある。これらの改訂内容は、PIV と直接関係のあるものではない。 しかしながら、実装については表 6 の 5 行目のバージョン番号の規定に従わなければならない。

表6: PIV 顔画像の INCITS 385 プロファイル

		節の表題および／またはフィールド名（かっこ内の番号は[FACESTD]の章番号）	INCITS 385-2004		PIV コンフォーマンス	備考
			フィールドまたは内容	必須値	許容値	
1.		バイト順(5.2.1)	NC		A	ビッグエンディアン
2.		数値(5.2.2)	NC		A	符号なし整数
3.	CBEFF	CBEFF ヘッダ (5.3)	MF	MV	パトロンフォーマット PIV	マルチフィールド CBEFF ヘッダ、第 6 節
4.	顔ヘッダ	フォーマット ID (5.4.1)	MF	MV	0x46414300	ASCII ″ FAC¥0″
5.		バージョン番号(5.4.2)	MF	MV	0x30313000	ASCII ″010¥0″
6.		レコード長(5.4.3)	MF	MV	MIT	注 1 を参照。
7.		顔画像数(5.4.4)	MF	MV	≥ 1	1 個以上の画像（K ≥ 1）注 2、3、および第 20 行を参照。
8.	顔情報。対象固有情報の単一インスタンス。	顔画像のブロック長(5.5.1)	MF	MV	MIT	
9.		特徴点数(5.5.2)	MF	MV	≥ 0	特徴数を計算した場合、正の値
10.		性別(5.5.3)	MF	OV	OIT	これらのフィールドは、政府機関の判断で意味のある値を、または指定しない場合は 0 を入れる。
11.		目の色(5.5.4)	MF	OV	OIT	
12.		髪の色(5.5.5)	MF	OV	OIT	
13.		特徴マスク (5.5.6)	MF	OV	OIT	

			節の表題および／またはフィールド名（かっこ内の番号は[FACESTD]の章番号）		INCITS 385-2004		PIV コンフォーマンス	備考
					フィールドまたは内容	必須値	許容値	
14.			表情(5.5.7)		MF	OV	1	ニュートラル
15.			ポーズの角度(5.5.8)		MF	OV	0	指定なしの場合は正面
16.			ポーズの角度の不確定性(5.5.9)		MF	OV	0	人による操作のため、正面
17.			MPEG4 の特性(5.6.1)		NC		OIT	
18.	特徴		顔の目鼻立ちの中心(5.6.2)		NC		OIT	
19.			顔の特徴ブロックコード化(5.6.3)		OF	OV	OIT	
20.			顔画像タイプ (5.7.1)		MF	MV	1	注 4 を参照。
21.			顔データタイプ (5.7.2)		MF	MV	0 または 1	注 5 を参照。圧縮アルゴリズム
22.			幅(5.7.3)		MF	MV	MIT	注 7 を参照。
23.			高さ(5.7.4)		MF	MV	MIT	
24.	画像情報。各インスタンスに画像固有の情報がある		画像の色空間(5.7.5)		MF	MV	1	sRGB。注 8 を参照。
25.			ソースタイプ (5.7.6)		MF	MV	2 または 6	デジタルスチール写真またはデジタルビデオ
26.			装置タイプ（ベンダー提供装置 ID）(5.7.7)		MF	MV	MIT	
27.			品質(5.7.8)		MF	MV	A	[FACESTD] では 0（無指定）
28.	画像データ		データ構造(5.8.1)		MF	MV	MIT	圧縮データ
29.	基本（第 6 節）	継承	継承(6.1)		NC		A	
30.			画像データコード化(6.2)		NC		A	注 5 を参照。
31.			画像データ圧縮(6.3)		NC		A	注 5 および注 6 を参照。
32.		フォーマット	顔ヘッダ（6.4.1）		NC		A	4 フィールドあり
33.			顔情報（6.4.2）		NC		A	9 フィールドあり
34.			画像情報（6.4.3）		NC		A	8 フィールドあり
35.	正面（第 7 節）		継承(7.1)		NC		A	基本継承
36.		シーン	目的（7.2.1）		NC		A	正面　附属書 A
37.			ポーズ（7.2.2）		NC		正面	±5 度
38.			表情（7.2.3）		NC		ニュートラル	
39.			顔位置調整の補助 (7.2.4)		NC		A	対象者のみが登場
40.			肩（7.2.5）		NC		A	体と顔をカメラに向ける
41.			背景（7.2.6）		NC		附属書 A.4.3	均一
42.			対象とシーンの照明（7.2.7）		NC		A	均一
43.			顔の影（7.2.8）		NC		A	なし
44.			眼窩の影（7.2.9）		NC		A	なし
45.			ホットスポット（7.2.10）		NC		A	ないこと。光を拡散させる。
46.			メガネ（7.2.11）		NC		A	対象者の通常の状態
47.			眼帯（7.2.12）		NC		A	医療用のみ
48.		写真	露出(7.3.2)		NC		A	飽和がないこと。
49.			ピントと被写界デプス (7.3.3)		NC		A	ピントが合っていること。
50.			不自然な色(7.3.4)		NC		A	ホワイトバランス
51.			カラーまたはグレースケールの強調(7.3.5)		NC		A＋再圧縮がないこと	後処理がないこと。
52.			カメラレンズの歪み (7.3.6)		NC		A＋附属書 A.8 による	
53.		デジタル	ジオメトリ	アスペクト比（7.4.2.1）			A	1 対 1 ピクセル
54.				原点（7.4.2.2）			A	左上が(0, 0)
55.			カラープロ	色密度(7.4.3.1)	NC		A	グレーで 7 ビットのダイナミックレンジ

			節の表題および／またはフィールド名（かっこ内の番号は[FACESTD]の章番号）		INCITS 385-2004		PIV コンフォーマンス	備考
					フィールドまたは内容	必須値	許容値	
56.			ファイル	彩度 (7.4.3.2)	NC		A	グレースケールで 7 ビットのダイナミックレンジ
57.				色空間(7.4.3.3)	NC		24 ビット RGB	オプション a、上記の色空間フィールドで報告。注 8 を参照。
58.			ビデオインタレース (7.4.4)		NC		A	インタレース式のセンサーは不可
59.	完全な正面画像（第 8 節）		継承(8.1)		NC		A	正面＋基本を継承
60.			シーン(8.2)		NC		A	正面＋基本を継承
61.		写真	中央に置いた画像(8.3.2)		NC		A	鼻を垂直中心線上に置く。
62.			目の位置(8.3.3)		NC		A	水平中心線より上とする。
63.			頭部の幅(8.3.4)		NC		A	注 7 を参照。
64.			頭部の長さ (8.3.5)		NC		A	注 7 を参照。
65.		デジタル	解像度(8.4.1)		NC		CC ≥ 240	注 7 を参照。
66.		フォーマット	継承(8.5.1)		NC		A	
67.			画像情報(8.5.2)		NC		A	
表の終り								

略語		意味
FAC	顔情報レコード	顔ヘッダ＋顔情報＋（画像情報＋画像データ）の繰り返し
MF	必須フィールド	[FACESTD]では、FAC にフィールドがなければならない
OF	オプションフィールド	[FACESTD]では、レコード内にフィールドがあることを許容する
MV	必須値	[FACESTD]では、フィールドに意味のある値がなければならない。
OV	オプション値	[FACESTD]では、意味のある値または「未指定」を示す 0 を許容する。
NC	規定の内容	[FACESTD]には、PIV に関する規定の慣例が示される。かかる節では、FAC 内にフィールドを定義しない。
A	必要に応じて	PIV の場合、値や慣例は[FACESTD]に規定されたとおりである。
MIT	インスタンス化時に必須	PIV の場合、レコードのインスタンス化時に決定される必須値。[FACESTD]に規定されている慣例に従う。
OIT	インスタンス化時に任意	PIV の場合、レコードのインスタンス化時に決定できる任意指定のヘッダ値。

規定についての注意:

1. 顔画像を PIV カードに保存する場合、レコード全体の長さは[800-73]が規定するコンテナーサイズの制限内に収まらなければならない。これらの制限は、[FACESTD]レコードだけでなく、CBEFF で格納された署名済みエンティティ全体に適用される。鍵の長さと署名アルゴリズムは[800-78]に規定されている。デジタル署名のサイズは鍵の長さによって増減し、バイオメトリックレコードのサイズでは変わらない。
2. 1 つのレコードに複数の画像を保存することができる。外見が時とともに変化する場合（髭の有無など）や再発行のために画像を収集する場合は、いくつかの画像を保存するのが適切な場合がある。最新の画像が最初に現れるようにし、これを申請時のデフォルトにしなければならない。
3. 顔画像を PIV カードに保存する場合、保存する画像は 1 画像のみでなければならない。
4. PIV 顔画像は、[FACESTD]第 8 節で規定する完全な正面画像タイプに適合しなければならない。
5. 顔画像データは、[FACESTD]第 6.2 節で列挙する圧縮フォーマットのいずれかでフォーマットしなければならない。画像全体を圧縮しても、または単一の関心範囲（ROI）だけを圧縮してもよい。本文書（[800-76]）では、新たに収集した顔画像は ISO/IEC 15444（つまり JPEG 2000）を使用して圧縮することを推奨する。これは、認証のために自動顔認識製品に画像を入力する場合、および画像を PIV カードに保存する場合に適用する。後者の

場合は、ROI 圧縮を用いなければならない。従来の ISO/IEC 10918 規格（つまり JPEG）の使用は、従来の画像のみに限らなければならない。

6. 顔画像の圧縮比は 15:1 以下でなければならない。ただし顔画像を PIV カードに保存する場合、ROI 圧縮には JPEG 2000 を使用しなければならない。最も内側の領域を顔の中心位置に置き、24:1 以下の圧縮比で圧縮する。
7. 顔認識の性能は、画像の空間分解機能に依存する。[FACESTD]では、完全正面画像タイプに対する最小解像度を規定していない。PIV の場合、1.5m の範囲にあるカメラに向かって幅 20cm の被写体を光軸に対し垂直に置いた状態で、その被写体が 240 ピクセル以上となる条件で顔の画像を取得しなければならない。これによって、頭部の幅（つまり、[FACESTD]の図 8 に示す「CC」の寸法）が、PIV カード上に印刷される顔の要素に対して十分な解像度を持つことが保証される。本仕様および[FACESTD]第 8.3.4 節は、画像の幅が 420 ピクセルを超えなければならないことを示している。この解像度仕様は、デジタル補間を行わずに光学的に得られなければならない。カメラから被写体までの距離は 1.5m 以上でなければならない（[FACESTD、附属書 A.8]に示した歪みのため）。このサイズ仕様は最小限の規定である。画像を自動顔認識に使用する場合、解像度が高いほど誤り率が下がると考えられる。
8. 顔画像データを保存する際には、画像データを sRGB 色空間に変換しなければならない。[FACESTD]第 7.4.3.3 節の記述どおり、これには使用中のカメラに使用するカラープロファイルを適用する必要がある。

6. PIV バイオメトリックデータの共通ヘッダ

PIV バイオメトリックデータはすべて、バイオメトリック共通データ交換フォーマット[CBEFF]に適合したデータ構造に組み込まなければならない。これは、すべてのバイオメトリックデータがデジタル署名され、画一的にカプセル化されなければならないことを規定している。その対象範囲には、[FIPS]が要求する PIV カードの指紋データ、政府機関が PIV カードに入れることを選択したその他のバイオメトリックデータ、政府機関が保持することを選択したバイオメトリックレコード（完全に独自の要素や派生的な要素を含む）、政府機関や登録機関により、またはそのために保持されるバイオメトリックデータが含まれる。第 3.6 節で述べた EFTS トランザクションデータは除外する。

上記のデータはすべて、必須バイオメトリック要素を[FIPS 201]および[800-73]の規定と同じ形式で署名しなければならない。この署名は完全性を保つために存在するもので、CBEFF 署名ブロック内に保存されなければならない。全体的な関係を整理して表 7 に示す。

表7: 簡略化した CBEFF の構造

CBEFF STRUCTURE		
CBEFF_HEADER	CBEFF_BIOMETRIC_RECORD	CBEFF_SIGNATURE_BLOCK
第 6 節	第 3.3 節、第 3.5 節、および第 5.2 節	FIPS 201
INCITS 398 5.2.1	INCITS 398 5.2.2	INCITS 398 5.2.3

表 8 で規定する CBEFF ヘッダとその注記は、NIST によりパトロンフォーマット「PIV」として確立される。このフォーマットは、[CBEFF、第 6.2 章]の条項に従って正式なパトロンフォーマットとして確立される。これは、[FIPS]が要求する最終的なデータタイプと FASC-N フィールドを、パトロンフォーマット A[CBEFF、附属書 A]で与えられるフィールドのサブセットに追加する。これは、パトロンフォーマット A から独立した存在である。このフォーマットの全フィールドが必須である。

表8: パトロンフォーマット PIV 仕様

	パトロンフォーマット PIV フィールド（かっこ内の番号は[CBEFF]の章番号）	長さ バイト 数	PIV データ タイプ	PIV コンフォーマンス 必須値
1.	パトロンヘッダバージョン (5.2.1.4)	1	UINT	0x03
2.	SBH セキュリティオプション(5.2.1.1,	1	ビットフ	注 2 を参照。

	5.2.1.2)		ィールド	
3.	BDB の長さ	4	UINT	バイオメトリックデータ CBEFF_BIOMETRIC_RECORD の長さ（バイト数）
4.	SB の長さ	2	UINT	CBEFF_SIGNATURE_BLOCK の長さ（バイト数）。注 3 を参照。
5.	BDB フォーマット所有者(5.2.1.17)	2	UINT	注 4 を参照。
6.	BDB フォーマットタイプ (5.2.1.17)	2	UINT	注 5 を参照。
7.	バイオメトリック作成日付(5.2.1.10)	8		データタイプについては注 6 を参照。
8.	有効期間(5.2.1.11)	16		データタイプについては注 7 を参照。
9.	バイオメトリックタイプ (5.2.1.5)	3	UINT	注 8 を参照。
10.	バイオメトリックデータタイプ (5.2.1.7)	1	ビットフィールド	注 9 を参照。
11.	バイオメトリックデータの品質(5.2.1.9)	1	SINT	注 10 を参照。
12.	作成者(5.2.1.12)	18	注 6	データタイプについては注 11 を参照。
13.	FASC-N	25	注 7	データタイプについては注 12 を参照。
14.	Reserved for Future Use（将来の使用のために予約）	4		0x00000000
表の終り				

規定についての注意:

1. 符号なし整数は UINT と表記した。符号付き整数は SINT と表記した。複数バイトからなる整数はビッグエンディアンのバイト順でなければならない。

2. セキュリティオプションのフィールドには、2 つの値が許容される。「b00001101」は、バイオメトリックデータブロックがデジタル署名されてはいるが暗号化されていないことを、「b00001111」はデジタル署名され暗号化されていることを示す。PIV カード上の必須[MINUSTD]要素に対する値は、「b00001101」である。

   4 番目のビット（マスク 0x08）は、本文書の以前のバージョンに従って設定される。それぞれのケースで設定される 3 番目のビット（マスク 0x04）は、デジタル署名をメッセージ認証コードと区別するという[CBEFF, 5.2.1.2]の要件を実現する。2 番目のビット（マスク 0x02）は、暗号化が使用されていることを示す。最初のビット（マスク 0x01）は、デジタル署名が使用されていることを示す。デジタル署名の計算に関する仕様は[FIPS, 4.4.2] と[800-78]で説明している。

3. 電子署名は、表 7 の CBEFF_HEADER と CBEFF_BIOMETRIC_RECORD を連結したものに対して計算しなければならない。CBEFF_HEADER の構造は、表 8 に示すとおりである。このヘッダには、「SB(署名ブロック)の長さ」（4 行目）が含まれるが、この長さは、電子署名を計算する前には知ることができないことがある。この問題は、次のような二段階の計算を行うことによって解決できる場合がある: 最初に、ダミーの値を「SB の長さ」フィールドにセットして、署名を計算した後、正しい署名の長さを「SB の長さ」フィールドにセットして、最後に署名を再計算する。

4. 第 3.4節、第 3.5 節、および第 5 節で定義した指紋および顔画像のレコードのフォーマット所有者は、INCITSバイオメトリック技術委員会であるM1 を意味する「0x001B」としなければならない。それ以外については、[CBEFF, 5.2.1.17]を参照すること。

5. 上記で定義した指紋画像データのフォーマットタイプは 0x0401 でなければならない。必須の指紋特徴点テンプレートデータのフォーマットタイプは、0x0201 でなければならない。顔データのフォーマットタイプは 0x0501 でなければならない。PIV カード上のその他のバイオメトリックレコード、またはその他の方法で政府機関が保持するバイオメトリックレコードには、[CBEFF, 5.2.1.17]の手順に従って値を割り当てなければならない。

6. これはバイオメトリックサンプルを取得した日付である。処理済みのサンプル（たとえばテンプレート）の場合、このデータはその親サンプルの取得日でなければならない。作成日は、「YYYYMMDDhhmmssZ」というバイナリー表現で 8 バイトのコード化をしなければならない。2 文字の組み合わせ（たとえば「DD」）を、符号なし整数として 8 ビットでコード化する。これにより、2005 年 12 月 15 日の 17:35:30 は「00010100 00000101 00001100 00001111 00010001 00100011 00011110 01011010」として表現される。ここで最後のバイトは ASCII 文字「Z」の

2 進表現で、時刻を世界標準時（UTC）で表していることを示すために含まれる。「hh」フィールドは、24 時間制による時刻をコード化しなければならない。1 つのレコードに複数のサンプル(たとえば、単指の特徴点画像が 2 つ)が含まれていて、作成日が異なる場合、最も早い日付を作成日とする。

7. 有効期間には 2 つの日付が含まれるが、これは上記第 6 項に従ってコード化しなければならない。
8. 指紋画像や各種指紋テンプレートのタイプは 0x000008、顔画像のタイプは 0x000002 としなければならない。その他のバイオメトリック方式の値は、[CBEFF, 5.2.1.5]で与えられるものでなければならない。[CBEFF, 5.2.1.5]に記載されていない方式の値は、0x0 でなければならない。
9. [CBEFF, 5.2.1.7]では、バイオメトリックデータの処理の程度によって 3 つのカテゴリを規定している。これらは表 9 でコード化される。必須の[MINUSTD] PIV カードテンプレートに対する値は、b100xxxxx でなければならない。

表9: CBEFF バイオメトリックデータタイプのコード化

データタイプ	PIV 必須値	カテゴリに含まれるバイオメトリックデータの例
生	b001xxxxx	[FACESTD] 画像および [FINGSTD] 画像
中間	b010xxxxx	
処理済	b100xxxxx	[MINUSTD] テンプレート

10. 単指の[FINGSTD]指紋画像、またはこれから抽出された[MINUSTD]テンプレートの品質値は Q = 20*(6 - NFIQ）でなければならず、NFIQ は[NFIQ]の方法で計算する。バイオメトリクスの複数の画像やサンプルがレコード内に含まれる場合、その最大値（すなわち最良値）をレポートしなければならない。PIV カードに保存されているか政府機関が保持しているかにかかわらず、バイオメトリックデータの品質値はすべて INCITS 358 の記述に従って、-2～100 の符号付き整数で表現しなければならない。−2 という値は実装が割り当てをサポートしていないことを示し、-1 は品質値を計算しようとして失敗したことを示さなければならない。0～100 の値は、数字が大きいほど最終的にサンプルが照合しやすいことを示す。[FACESTD]の要件によるゼロ値はこの CBEFF フィールドでは-2 としてコード化される。
11. PIV では、作成者フィールドは 18 バイトの長さを持ち、最初の K バイト（K は 17 以下）は印字可能な ASCII 文字で、残り（18－K）バイトの最初のバイトはヌル終端（ゼロ）でなければならない。
12. このフィールドは、[800-73, 1.8. {3,4}]に従って CHUID 識別子の FASC-N コンポーネントを 25 バイト含まなければならない。

7. 性能試験および認証手続き

7.1 適用範囲

この節では、[FIPS]が規定する必須バイオメトリック要素、すなわち PIV カード上に置かれた 2 個の指紋特徴点テンプレートの生成や一致を行う実装の認証に使用されるテストの標準的な仕様を規定する。本節では、テストそのものと、テストを実施する機関を規定するものであり、試験対象物(被験品)は規定しない。また、ここで述べるデータ仕様と、第 3 節に記載の現場に実装する PIV 認証のデータ仕様を混同してはならない。取り扱う範囲に関する詳細は、第 7.6 節を参照のこと。

7.2 PIV 認証

これらのテンプレートは、第 3.4 節で概略を述べたように[MINUSTD]に適合する。[800-73、付録 C]のユースケースには、テンプレートや PIV カードを使用して相互運用可能な認証を行う方法が詳しく説明されている。認証には PIV カードテンプレートの一方または両方を使用する。これらのテンプレートは、第 1 指または第 2 指（または両方）の新たに取得された（つまり、ライブの）指紋画像と照合される。[MINUSTD]ヘッダに指の位置を含めると、ユーザーに特定の指（1 本または複数本）の入力を求めるプロンプトが表示できる。

認証性能は、本人拒否率（FRR）と他人受入率（FAR）の両方の観点から定量化される。FRR は、PIV で正当なカード保有者が誤ってアクセスを拒否される比率を定量化し、後者は詐称者が誤ってアクセスを許可される比率を定量化する。この誤り率は、環境、試行回数（センサー上に指を置く回数）、センサー自体、PIV カードテンプレートの親画像の品質、チェックした指紋数、ユーザーのプロセス習熟度など多くの要因に依存する。すべての認証トランザクションで 2 本の指を使う場合、単指での認証と照合して大幅に性能が向上する。相互運用可能なバイオメトリックの[FIPS]仕様は、ベンダー間および政府機関間での PIV カード認証をサポートすることを意図したものである。この複数の見方が、性能のばらつきの原因となる。

7.3 試験の概要

この節では、[MINUSTD]テンプレートの生成プログラムと照合プログラムの認証手順を規定する。

操作の相互運用性の試験では製品間のテンプレート交換が必要なので、グループとして試験しなければならない。そのため、試験機関はまず 1 ラウンド目の試験で、相互運用可能なテンプレート生成プログラムと照合プログラムの一次グループを確立しなければならない。認証は、試験終了時に定量的に判定しなければならない。その後の認証では、以前に認証された製品との相互運用性が求められる。

認証手順はオフラインで行わなければならない。これにより、非常に大量のバイオメトリックデータを使用して、再現可能で決定論的な、したがって監査可能な評価によって製品が認証できる。相互運用可能なあらゆる製品の組の間でテンプレートデータを交換するときの性能の測定には、オフライン評価が必要である。サンプルの差による性能への影響を定量化するためには、母集団が大きくなければならない。テンプレート生成プログラムは、論理的には画像からテンプレートへのコンバータである。テンプレート照合プログラムは、1～2 枚の認証テンプレートを 1～2 個の登録テンプレートと論理的に照合して、類似度得点を発生させる。テンプレート生成プログラムとテンプレート照合プログラムは別々に認証しなければならない。この考え方は以下の理由による。

1. テンプレートの生成はその手順から見ても、アルゴリズムから見ても、あるいは物理的にも照合プロセスとは区別されるものである。
2. テンプレート生成は[FIPS]の要求であるが、照合はそうではない。
3. 指紋テンプレート操作の相互運用性は、PIV カードテンプレートの品質に依存する。サプライヤが高性能な生成プログラムと高性能な照合プログラムを両方とも製造しなければならないとすれば、相互運用可能なテンプレートの完全なメリットは実現できないと考えられる。

4. テンプレート生成プログラムが認証されて導入されると、生成されたテンプレートが出回るようになる。すべての照合プログラムが、これらのテンプレートを処理できなければならない。生成プログラムと照合プログラムが一緒に認証されると、その後の認証ラウンドは複雑になる。

別々に認証を行うという意味は、サプライヤがそれぞれ 1 個以上のテンプレート生成プログラムと 0 個以上の照合プログラムを認証用に提出することがあるということである。最終的には、提出された 1 個以上の製品が認証される。

この試験計画は、本文書でその概要を紹介した現在草案段階の ISO/IEC 19795-4 [ISOSWAP]規格の規定に適合する。この規格の要件の 1 つは、試験をブラインドで行わなければならないことである。PIV テストにおいて、テンプレート照合プログラムは登録テンプレートのソースが認識できない。

7.3.1 テンプレート生成プログラム

テンプレート生成プログラムは、ソフトウェアライブラリとして認証されなければならない。テンプレート生成プログラムは、PIV で画像を特徴点レコードに変換するライブラリ機能である。入力画像は、PIV への登録平面押捺を表す。出力テンプレートは、PIV カードテンプレートを表す。サプライヤが認証用に提出する実装は、試験主催者が公表する API(Application Programming Interface)仕様の要件を満足しなければならない。この API 仕様は、テンプレート生成プログラムに対して、画像データを受け入れて表 11 に適合する[MINUSTD]テンプレートを生成することを求めるものである。表 11 にその値や慣例が明確に述べられていない場合、第 3.4.2 節および表 3 の仕様が適用される（たとえば、特徴点のタイプ）。CBEFF ヘッダと CBEFF 署名は含めてはならない。

試験機関は、表 11 のオプション A のデータ要素仕様またはオプション B のデータ要素仕様のいずれかを用いて、画像をテンプレート生成プログラムに入力しなければならない。入力データは、試験機関が用意しなければならない。

テスト仕様では、テンプレート生成プログラムに対して、入力が何であっても適合するテンプレートを生成することを求めるべきである。かかるテンプレートには、特徴点がない場合がある。この規定は、透過的かつ正確に登録の失敗を明らかにする。導入されるシステムでは、品質評価や画像解析アルゴリズムによって入力データが一致しないと判定された場合、登録の失敗が宣言されることがある。オフライン試験では、そのような判定がなされた場合、少なくとも特徴点のないテンプレートが生成されなければならない。ただし、PIV では他サプライヤの照合プログラムであればさらに劣悪なテンプレートでも扱える場合があるため、試験用に提出されるテンプレート生成プログラムは内部的な品質承認の仕組みを重視するのではなく、使用可能なテンプレートの生成に努めるべきである。

表10: INCITS 381 PIV カードテンプレート生成プログラム認証への入力仕様

必須のデータ要素		PIV 認証値	参考
オプション A: 解析済み INCITS381 コンテナ － テンプレート生成プログラムの関数呼び出しに使用するパラメタ。			
1.	指紋画像データ	MIT	非圧縮ピクセルデータ、左から右、上から下へピクセル当たり 1 バイト（8 ビット）で保存。画像のバイト数はピクセル単位の高さに幅を乗じた値に等しい。
2.	指紋画像の画質	20,40,60,80,100	[NFIQ]に不合格の指紋は認証試験には使用しない。 これらの値は[MINEX]に使用する値とは異なる。
3.	指の位置	MIT	
4.	押捺タイプ	0	
5.	垂直線の長さ	MIT	高さ
6.	水平線の長さ	MIT	幅
オプション B: 解析されていない INCITS381 コンテナ			
1.	フォーマット ID (7.1.1)	0x46495200	ASCII ″FIR¥0″
2.	バージョン番号(7.1.2)	0x30313000	ASCII ″010¥0″
3.	レコード長(7.1.3)	MIT	
4.	CBEFF 製品 ID (7.1.4)	0	
5.	取り込み装置 ID (7.1.5)	0	
6.	画像取得レベル I (7.1.6)	30 または 31	
7.	画像数(7.1.7)	1	

	必須のデータ要素	PIV 認証値	参考
8.	尺度の単位(7.1.8)	0x02	1 センチ当たりのピクセル数
9.	スキャン解像度(水平)(7.1.9)	197	
10.	スキャン解像度(垂直) (7.1.10)	197	
11.	画像解像度(水平) (7.1.11)	197	
12.	画像解像度(垂直)(vert) (7.1.12)	197	
13.	ピクセルデプス (7.1.13)	8	
14.	画像圧縮アルゴリズム (7.1.14)	0	非圧縮
15.	予備(7.1.15)	0	2 バイト、表 4 の下の注 12 を参照。
16.	指紋データのブロック長(7.2.1)	MIT	
17.	指の位置(7.2.2)	MIT	
18.	表示の数(7.2.3)	1	
19.	表示番号(7.2.4)	1	
20.	指紋画像の画質(7.2.5)	20,40,60,80,100	[NFIQ]に不合格の指紋は認証試験には使用しない。 これらの値は[MINEX]に使用する値とは異なる。
21.	押捺タイプ (7.2.6)	0	ライブスキャンによる平面押捺のみ
22.	水平線の長さ (7.2.7)	MIT	
23.	垂直線の長さ(7.2.8)	MIT	
24.	予備(FINGSTD, 表 4)	0	1 バイト、表 4 の下の注 11 を参照。
25.	指紋画像データ (7.2.9)	MIT	非圧縮ピクセルデータ、左から右、上から下へピクセル当たり 1 バイト (8 ビット)で保存。画像のバイト数はピクセル単位の高さに幅を乗じた値に等しい。
表の終り			

表11: INCITS 378 PIV カードテンプレート生成プログラムおよび PIV テンプレート照合プログラムの認証仕様

	節の表題および／またはフィールド名 (かっこ内の番号は[MINUSTD]の章番号)	PIV 許容適合値	参考
1.	フォーマット ID (6.4.1)	0x464D5200	ASCII ″FMR¥0″
2.	バージョン番号(6.4.2)	0x20323000	ASCII ″ 20¥0″.
3.	レコード長(6.4.3)	26 ≤ L ≤ 800	26 バイトのヘッダ、最大 128 個の特徴点 18 行目を参照。
4.	CBEFF 製品 ID の所有者(6.4.4)	0	
5.	CBEFF 製品 ID タイプ (6.4.4)	0	
6.	取り込み装置のコンフォーマンス (6.4.5)	0	
7.	取り込み装置 ID (6.4.6)	0	
8.	スキャン画像の x 方向のサイズ (6.4.7)	MIT	入力データから直接継承
9.	スキャン画像の y 方向のサイズ (6.4.8)	MIT	
10.	X(水平)方向の解像度(6.4.9)	197	
11.	Y(垂直)方向の解像度(6.4.10)	197	
12.	指表示の数(6.4.11)	1	
13.	予備バイト (6.4.12)	0	
14.	指の位置(6.5.1.1)	MIT	入力データから直接継承
15.	表示番号(6.5.1.2)	0	
16.	押捺タイプ(6.5.1.3)	0 または 2	入力データから直接継承
17.	指の画質(6.5.1.4)	MIT	入力データから直接継承
18.	特徴点の数(6.5.1.5)	0 ≤ M ≤ 128	M 個の特徴点データレコードが続く。

	節の表題および／またはフィールド名 （かっこ内の番号は[MINUSTD]の章番号）	PIV 許容適合値	参考
19.	特徴点のタイプ（6.5.2.1）	01b, 10b または 00b	表 3 の下の注 1 を参照。
20.	特徴点の位置(6.5.2.2)	MIT	表 3 の下の注 7 を参照。
21.	特徴点の角度(6.5.2.3)	MIT	表 3 の下の注 8 を参照。
22.	特徴点の画質(6.5.2.4)	0	
23.	拡張データのブロック長(6.6.1.1)	0	このフィールドの後ろにバイトを含めてはならない。
表の終り			

略語		意味
MIT	インスタンス時に必須	PIV 認証の場合、レコードのインスタンス化時に決定される必須値。[FINGSTD]に規定されている慣例に従わなければならない。

7.3.2 テンプレート照合プログラム

テンプレート照合プログラムは、ソフトウェアライブラリとして認証されなければならない。PIV の場合、照合プログラムは登録テンプレートを認証テンプレートと照合して類似度得点を発生させるソフトウェア機能である。類似度得点は、整数または実数で表される量でなければならない。登録テンプレートは、PIV カードテンプレートを表す。認証テンプレートは、ライブで取得された認証指紋から抽出されたテンプレートを表す。サプライヤが認証用に提出する実装は、試験主催者が公表する API 仕様を満足しなければならない。

この API 仕様は少なくとも 1 つの認証テンプレート (対象者の第 1 指と第 2 指から得られたもの)と 1 つの登録テンプレート（対象者または別人の同じ指から得られたもの）の照合をサポートする。二つのテンプレートは、表 12 に示す[MINUSTD]のプロファイルに適合しなければならない。

このガイドラインでは、指紋を基本的な照合に使用する方法について、指示も禁止もしない。ここでの制約は、照合機能が呼び出されると、入力テンプレートによらず類似度得点を出力しなければならないということだけである。得点が多いほど、入力データが本人のものである可能性が高いことを示すものと解釈されなければならない。入力に対する照合に失敗または拒否された場合でも、常に得点を出力しなければならない。本文書では、その場合低い得点を報告することを実装者に推奨する。

入力する[MINUSTD]登録テンプレートは、試験機関がサプライヤのソフトウェアを使用して準備しなければならない。入力する[MINUSTD]認証テンプレートは、テスト対象のテンプレート照合プログラムのサプライヤが提供する、テンプレート生成ソフトウェアにより出力されたものでなければならない。

7.4 試験手順

試験機関は、試験仕様書を公表しなければならない。この文書で、認証を受けるための製品の提出期限を規定しなければならない。

テンプレート生成プログラムのサプライヤは、試験機関に認証依頼を提出しなければならない。試験機関は、これらのサプライヤにサンプル一式を与えなければならない。このサンプル一式はデバッグ作業をサポートするもので、表 10 の仕様 A または仕様 B に適合した画像を含まなければならない。サプライヤは、このデータから得られたテンプレートを試験機関に提出しなければならない。サプライヤは、テンプレート生成プログラムを試験機関に提出しなければならない。試験機関はそのテンプレート生成プログラムを実行して、サプライヤが提出したものと同じテンプレートが作成されることを確認しなければならない。試験機関は、コンフォーマンス評価プログラムをテンプレートに適用しなければならない。試験機関は、同一のテンプレートが得られたかどうか、およびテンプレートが表 11 の仕様に適合しているかどうかをサプライヤに報告しなければならない。この妥当性確認プロセスは反復可能である。

テンプレート照合プログラムのサプライヤは試験機関に認証依頼を提出する。試験機関は、これらのサプライヤにサンプル一式を与えなければならない。このサンプル一式はデバッグ作業をサポートするもので、表 10 の仕様 A または仕様 B に適合した画像、および表 11 の仕様に適合したテンプレートを含まなければならない。サプライヤは、このデー

タから得られた類似度得点を試験機関に提出しなければならない。サプライヤは、テンプレート照合プログラムを試験機関に提出しなければならない。試験機関はこの照合プログラムを実行して、サプライヤが提出したものと同じ得点が得られることを確認しなければならない。試験機関は、サプライヤに確認結果を報告しなければならない。この妥当性確認プロセスは反復可能である。

試験機関は、試験本体のすべてのメンバーから得られた最初のバイオメトリックサンプルを、すべてのテンプレート生成プログラムに適用しなければならない。試験機関は、すべてのテンプレート照合プログラムを呼び出して、生成された登録テンプレートと試験本体のすべてのメンバーから得られた 2 番目の認証テンプレートを照合しなければならない。認証テンプレートは、照合プログラムのサプライヤの生成プログラム（つまり、他のサプライヤの生成プログラムではない）よって生成されたものでなければならない。これを、テンプレート生成プログラムとテンプレート照合プログラムの対となるすべての組み合わせについて行わなければならない。その結果、それぞれの組み合わせに対して真正な（本人の）類似度得点のセットが得られる。

試験機関は、すべてのテンプレート照合プログラムを呼び出して、登録テンプレートと、共通メンバーを持たない母集団のメンバーから得られた 2 番目の認証テンプレートを照合しなければならない。認証テンプレートは、あらゆるケースにおいて、照合プログラムのサプライヤの生成プログラムによって生成されるべきである。これを、テンプレート生成プログラムとテンプレート照合プログラムの対となるすべての組み合わせについて行わなければならない。その結果、それぞれの組み合わせに対して詐称者の類似度得点のセットが得られる。本人の得点と詐称者の類似度得点が生成される順番はランダム化し、その順番は最後の 2 パラグラフの順番から推測できるものであってはならない。

試験機関は、第 1 指の画像を照合して得られた類似度得点と第 2 指の画像を照合して得られた得点の合計を計算しなければならない。この総和則の融合は、2 本指認証を象徴するプロセスである。

7.5 相互運用可能グループの決定

試験機関は、テンプレート生成プログラムとテンプレート照合プログラムの対となるすべての組み合わせについて、検出誤りトレードオフ特性（DET）を計算しなければならない。試験機関は、相互運用可能性の矩形行列を生成しなければならない（[ISOSWAP]参照）。この行列は、行が生成プログラムに、列が照合プログラムに対応する。相互運用性行列の各要素は、ある他人受入率（FAR）での本人拒否率（FRR）である。この値は、DET 上の 1 つの動作点に対応する。第 7.3.1 節に示したとおり、DET には登録や取得の失敗の影響が自動的に含まれる。

相互運用可能なテンプレート生成プログラムおよび照合プログラムのグループは、FAR 動作点を 1%に固定した時の相互運用性サブマトリクスの全要素（すなわち FRR 値）が 1%以下となる、初期認証ラウンドに提出されたグループのうちで、最大のサブグループでなければならない。すべての対になる製品の組み合わせが、このしきい値を下回らなければならないという条件は、PIV アプリケーションが相互運用性の保証されない分離した組み合わせを許容しないことから設定されたものである。

7.6 PIV におけるバイオメトリックシステムのパフォーマンス

第 7 節のテストは、基本的な特徴点ベースの相互運用可能性を立証できる製品を特定することのみを目的としたものである。特に、第 7.5 節で述べた誤り率の仕様は、このテストを通じて特徴点の生成と照合プログラムの有効性を確立するためだけのものである。実際に、バイオメトリック製品（指紋特徴点ベースの製品、またはそのほかをベースにした製品）の利用に関しては、以下の項目は本規格では規定していない:

- 現場に実装するバイオメトリックシステムの誤り率に関する仕様の決定。
- 複数サンプル（たとえば、2 本の指）の使用を求めること。
- 政府機関が、本人拒否率（FRR）と他人受入率（FAR）に対する運用時のしきい値を、本書第 7.5 節で規定している値（たとえば、FAR=0.4%、または FRR=1.25%）とは異なる目標値に設定することを禁止すること。
- 政府機関が独自の補足試験を実施することを禁止すること。これらは、単一製品の性能試験または相互運用性の試験であることが考えられ、アプリケーション固有の性能を測定するために利用されることがある。

一般的にシステムの性能は、組織の利用方針（たとえば、試行回数を 3 回に設定）、認証に使用する指の数（たとえば、1 本、場合によっては 2 本）、環境的要因（たとえば、湿度）、画質、および母集団の影響（たとえば、年齢）などのさ

まざまな要因によって変化するため、このテストで測定された精度と現場に実装するシステムの精度とは異なる場合があることに注意すること。

[redacted]

8. 本仕様へのコンフォーマンス

8.1 コンフォーマンス

実装およびその関連データレコードが、規定(「ねばならない」)節である第 3 節～第 6 節に適合すれば、本仕様へのコンフォーマンスが達成される。以下は、この記述を要約したものである。

8.2 PIV 登録指紋取得仕様へのコンフォーマンス

第 3.2 節に適合するには、完全な指紋画像一式を収集するための[EFTS、付録 F]認証を受けたスキャナの使用、セグメント化アルゴリズムおよび[NFIQ]に基づいた品質保証手続きの適用が必要である。画像が本仕様に適合するには、以下の条件を満足しなければならない。

1. 第 3.2 節の取得手順に従っていること。これは人が観測することにより試験できる。
2. 画像が表 4 およびその規定についての注意で概略を示したとおり、[FINGSTD]に適合していること。

8.3 PIV カード指紋テンプレートレコードへのコンフォーマンス

第 3.4 節へのコンフォーマンスは、その節の中のすべての規定の内容に適合することにより実現できる。これには、第 3.4 節で概略を述べた[MINUSTD]に適合するレコードの作成も含まれる。コンフォーマンスは、レコードの検査および表 3 の「PIV コンフォーマンス」列の試験表明を実行することにより試験しなければならない。第 7 節に従った性能の認証が必要である。

8.4 政府機関が保持する PIV 登録指紋のコンフォーマンス

第 3.5 節へのコンフォーマンスは、その節の中のすべての規定の内容に適合することにより実現できる。これには、第 3.5 節で概略を述べた[FINGSTD]に適合するレコードの作成も含まれる。コンフォーマンスは、レコードの検査および表 4 の「PIV コンフォーマンス」列の試験表明を実行することにより試験しなければならない。品質値[NFIQ]は、NIST のリファレンス実装と対照して確認しなければならない。

8.5 PIV 身元調査レコードのコンフォーマンス

第 3.6 節へのコンフォーマンスは、その節の中のすべての規定の内容に適合することにより実現できる。そのため、身元調査に対する FBI の規定要件に適合する必要がある。これは FBI に提出されたトランザクションの検査によって試験しなければならない。この検査は、提出政府機関または FBI のいずれかでトランザクションを捕捉することにより行える。

8.6 PIV 認証指紋取得仕様へのコンフォーマンス

第 4.2 節へのコンフォーマンスは、[SINGFING]に従った認証が得られ、解像度と面積の仕様が満足されれば達成される。[SINGFING]認証プロセスは、出力画像の検査を必要とする。

8.7 PIV 顔画像レコードのコンフォーマンス

第 5 節へのコンフォーマンスは、その節の中のすべての規定の内容に適合することにより実現できる。これには、第 5.2 節で概略を述べた[FACESTD]に適合するレコードの作成も含まれる。コンフォーマンスは、レコードの検査および表 6 の「PIV コンフォーマンス」列の試験表明を実行することにより試験しなければならない。

8.8 CBEFF 格納のコンフォーマンス

本文書または[FIPS]で要求されているかどうかにはかかわらず、すべてのバイオメトリックデータレコードが適合 CBEFF レコードにカプセル化されていれば、その PIV システムは第 6 節に適合する。CBEFF レコードは、以下の条件が満足されていれば適合する。

1. 表 8 のヘッダのフィールドが存在すること。
2. 表 8 のフィールドに、その規定についての注意に示された許容値が含まれていること。
3. [800-78]に適合するデジタル署名が存在すること。
4. 値が、そこに含まれるバイオメトリックデータおよび後続のデジタル署名と整合していること。

PIV バイオメトリックデータのコンフォーマンスを試験するためのアプリケーションは、デジタル署名を解読し確認するための適切な鍵とともに提供されなければならない。

8.9 テンプレート生成プログラムのコンフォーマンス

テンプレート生成プログラムは、その出力と計算速度のコンフォーマンス、および生成されたテンプレートが第 7 節に適合する相互運用性の試験で照合されたときに得られる誤り率に基づいて認証される。

テンプレート生成プログラムは、以下の条件を満足することにより認証される。

1. 表 10 に示すすべての[FINGSTD]入力インスタンスを表 11 に示す[MINUSTD]テンプレートに変換し、それらが NIST の規定するテンプレートコンフォーマンス試験一式に合格すること。
2. 表 10 の[FINGSTD]インスタンスの 90%を 1.3 秒 未満 [4]で変換すること。
3. 認証されたすべての照合プログラムの FAR を 1%に設定して、出力テンプレートを照合した際に、FRR 値が 1%以下になること。

8.10 テンプレート照合プログラムのコンフォーマンス

テンプレート照合プログラムは、その計算速度、およびテンプレートが第 7 節に適合する相互運用性の試験で照合されたときに得られる誤り率に基づいて認証される。

テンプレート照合プログラムは、以下の条件を満足することにより認証される。

1. 表 11 の [MINUSTD] 入力テンプレートをすべてスカラー量で表現される得点に変換すること。
1. 第 7.4 節のテンプレート照合の 90%を 0.1 秒未満 [4] で実行すること。
2. テンプレート照合プログラムの FAR を 1%に設定して、認証されたすべてのテンプレート生成プログラム、および当該照合プログラムが付属する生成プログラムによって生成されたテンプレートを照合した際に、FRR 値が 1%以下になること。

[4] 本仕様は、2005 年に調達され 2GHz のプロセッサと 512MB のメインメモリーを備えた市販 PC に適用される。本仕様は、計算機プラットフォームでの大きな変化を反映させるために、試験機関が調整しなければならない。

9. 参考文献

Citation	Document
800-73	NIST Special Publication 800-73-1, Interfaces for Personal Identity Verification
800-78	NIST Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification
CBEFF	INCITS 398-2005, American National Standard for Information Technology - Common Biometric Exchange Formats Framework (CBEFF)
EFTS	IAFIS-DOC-01078-7.1 CJIS-RS-0010 (V7.1) – Electronic Fingerprint Transmission Specification, Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice May 2, 2005。この文書は、http://www.fbi.gov/hq/cjisd/iafis.htm から入手できる。 http://www.fbi.gov/hq/cjisd/iafis/efts71/cover.htm にある資料は、最新ではない可能性がある。実装者は、EFTS の完全文書(FBIが提供する付録Nを含む)を要求すべきである。
FFSMT	ANSI/NIST-ITL 1-2000 – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, NIST Special Publication 500-245, 2000.
FINGSTD	INCITS 381-2004, American National Standard for Information Technology - Finger Image-Based Data Interchange Format
FIPS	FIPS 201, Personal Identity Verification, National Institute of Standards and Technology, 2005.
MINUSTD	INCITS 378-2004, American National Standard for Information Technology - Finger Minutiae Format for Data Interchange
FACESTD	INCITS 385-2004, American National Standard for Information Technology - Face Recognition Format for Data Interchange
ICS	Methods for Testing and Specification (MTS); Implementation Conformance Statement (ICS) Proforma style guide. EG 201 058 V1.2.3 (1998-04)
ISOSWAP	ISO/IEC 19795:2005 Information Technology — Biometric Performance Testing and Reporting — Part 4: Interoperability Performance Testing
MINEX	Minutiae Interoperability Exchange Test, Evaluation Report: NISTIR 7296 http://fingerprint.nist.gov/minex04
NFACS	IAFIS-DOC-07054-1.0, Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice, April 2004.
NFIQ	NISTIR 7151 - Fingerprint Image Quality, NIST Interagency Report, August 2004
SINGFING	"Personal Identity Verification (PIV): Image Quality Specifications For Single Finger Capture Devices"を参照. http://www.fbi.gov/hq/cjisd/iafis/piv/pivspec.pdf