NIST Special Publication 800-73-1

個人識別情報検証のインタフェース

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce
米国国立標準技術研究所
技術管理局
米国商務省

James F. Dray
Scott B. Guthery
Teresa Schwarzhoff

情　報　セ　キ　ュ　リ　テ　ィ

米国国立標準技術研究所
情報技術ラボラトリ
Gaithersburg, MD 20899-8930

2006 年 3 月

米国商務省　長官
Carlos M. Gutierrez

米国国立標準技術研究所　所長
William Jeffery

IPA 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

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、国の測定基準及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、連邦政府の情報タシステムにおいて、費用対効果の高いセキュリティと、国家的セキュリティに関連しない情報のプライバシーを確保するための技術的、物理的、管理的及び運用のための規格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、コンピュータセキュリティにおける情報技術ラボラトリの調査、ガイダンス、成果を報告し、産業界、政府機関及び教育機関との共同活動についても報告する。

本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体は本レポートに記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。
PIV は、本人の認証、情報へのアクセス制御、電子署名などを含んでいますが、支払い機能は含んでおりません。また、本文書の対象は米国連邦政府内で有効なクローズドシステムであり、その意味で、連邦政府特有の技術仕様を含んだ個別システムと言うことができます（但し、連邦政府内のすべての省庁では相互運用性のあるものという考え方に立っています）。PIV シリーズ文書の考え方には、我が国で、職員が施設へ入退室する際や情報へのアクセス制御を行う際の本人確認を IC カードで行おうとする場合に、参考にできる情報が多く含まれています。

米国国立標準技術研究所 Special Publication 800-73-1、71 ページ
（2006 年 3 月）

謝辞

本書執筆陣である NIST の James Dray、Terry Schwarzhoff および Mobile Mind, Inc.の Scott Guthery は、本書のドラフトをレビューし作成に貢献してくれた同僚に感謝の意を表したい。SP 800-73 の作成プロセスに詳細な技術情報を提供していただいた Government Smart Card Interagency Advisory Board（GSC-IAB）および情報技術規格国際委員会（INCITS:InterNational Committee for Information Technology Standards）には特にお礼を申し上げたい。Booz Allen Hamilton 社にも感謝しなければならない。特に Ketan Mehta 氏には、技術面および編集面で重要な貢献をしていただいた。さらに、公共および民間部門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。これらの思慮深い建設的なコメントによって、本書の質と実用性が高められた。

本書の日本語版作成にあたっては、
電子商取引安全技術研究組合　常務理事　植村泰佳様、
株式会社電子商取引安全技術研究所　顧問　廣川勝久様 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。

目次

図

表

1. パート 1:序論、PIV データモデル、および移行に関する考慮事項

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クレデンシャルの相互運用を管理する、共通の識別標準を採用することを要求していた。身元クレデンシャルに関する標準を確立するために、連邦情報処理規格 201『Personal Identity Verification (PIV) of Federal Employees and Contractors(連邦政府機関従業者および契約業者の個人識別情報検証)』(FIPS 201)[4]が策定された。本文書 (Special Publication 800-73 (SP 800-73)) は、PIV カード[1]から身元クレデンシャルを取得して使用するためのインタフェース要件を規定したものであり、FIPS 201 の関連文書である。

1.1 作成機関

本文書は、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 に基づくその法的責任を果たすために、米国国立標準技術研究所(NIST:National Institute of Standards and Technology)により作成された。

NIST は、すべての連邦政府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、最低要件を含んだ規格およびガイドラインを作成する責任があるが、このような規格およびガイドラインは国家安全保障関連の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)』の要件に一致しており、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。非政府組織が自己責任において使用することもでき、著作権の制約はないが、出自を明らかにすることが望ましい(翻訳者注:著作権に関するこの記述は、SP800-73 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 および NRI セキュアテクノロジーズ株式会社に帰属する)。本文書におけるいかなる記述も、商務長官が法的権限に基づき連邦政府機関に対して義務や拘束力を行使している標準および指針と矛盾するものととらえるべきではない。また、本勧告は、商務長官、行政管理予算局長、または他のいかなる連邦政府役人の既存の権威を変更したり、これらに優先するものと解釈すべきではない。

1.2 目的

FIPS 201 は、識別情報の検査、登録、PIV カードの発行、PIV カードの利用などの PIV ライフサイクル活動に関する手順を定義している。また、FIPS 201 は、身元クレデンシャルをスマートカードに保存しなければならないことも規定している。本文書は、身元クレデンシャルを取り出して利用するための、スマートカードとのインタフェースに関する技術仕様を含んでいる。これらの仕様は、相互運用性という設計目標と PIV カードの機能を反映したものである。この目標には、PIV データモデル、通信インタフェース、およびアプリケーションプログラミングインタフェースを規定することで取り組んでいる。また、この仕様は、標準に複数の選択肢や分岐が含まれる要件を列挙している。本文書では、規定標準を実装者が解釈する際の制約をさらに強めている。この制約は、PIV アプリケーションに適した方法で実装の容易さ、相互運用性の促進、およびパフォーマンスの保証のために策定したものである。

[1] 個人向けに発行される物理的な制作物(例えば、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、格納されている身元クレデンシャル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、身分クレデンシャル(例えば、写真、暗号鍵、バイオメトリクデータなど)が格納されているもの。

1.3 適用範囲

本文書は、各連邦政府機関で採用されている PIV の相互運用性を確保するために必須のユースケースに準拠するために必要となる、PIV データモデル、アプリケーションプログラミングインタフェース（API）、およびカードインタフェースの要件を規定する。なお、必須ユースケース(the mandated use cases)に関しては、FIPS 201 の 6 節で定義され、以下の 1.7 節でさらに詳しく記述されている。相互運用性とは、クライアントアプリケーションプログラム、標準に適合したカードアプリケーション、および標準に適合した IC カード（ICC）を、連邦政府機関同士のあらゆる情報処理システムと互換性を保ちながら使用できるように PIV 身元クレデンシャルを利用することであると定義されている。本仕様は、PIV データ要素の識別子、構造、および書式を定義する。本仕様は、PIV カードを使用するためのクライアントアプリケーションプログラミングインタフェースおよびカードコマンドインタフェースついても記述する。本文書では、識別情報の十分な正当性を確保するために実行されなければならないバックエンドプロセスについては取り上げていない。

1.4 対象読者と前提条件

本文書は、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。また、読者に、スマートカードの標準およびアプリケーションに関する実用上の知識があることを想定している。

1.5 文書の概要

本文書は、個人識別情報検証に関するクライアントアプリケーションプログラミングインタフェースおよびカードコマンドインタフェースの 2 つの実現形態、つまり、*暫定*インタフェース訳注：移行を前提としたカード仕様でのインタフェース 1.6 を参照のこと）と*最終*インタフェース（訳注：「FIPS 201 PIV–II カード仕様」のインタフェース。1.6 を参照のこと）について記述する。

既存の ID カードプログラムを持つ政府機関は、最終インタフェースへ発展させる際のオプションの中間段階として暫定インタフェースを使用できる。最終インタフェースは、既存の ID カードプログラムを持たない政府機関や、2 段階ではなく 1 段階で最終インタフェースへ発展させることを選択した政府機関が使用する。

本文書は、以下のような 3 つのパートに分かれている。

1.5.1 パート 1：共通データモデルと移行に関する考慮事項

パート 1 には、本文書の最初の節である第 1 節が含まれる。第 1 節では、本文書自体について説明するとともに、暫定インタフェースと最終インタフェースの両者に共通する仕様について記述している。また、暫定インタフェースから最終インタフェースへの移行戦略に関するガイダンスも含まれている。

暫定インタフェースと最終インタフェースのいずれにも、まったく同じデータが使用される。そのため、個人識別情報検証に関するデータ（PIV データモデル）の記述は、第 1 節に含まれる。

1.5.2 パート 2：暫定インタフェース

パート 2 には、本文書の第 2 節が含まれる。第 2 節では、GSC-IS に基づいたレガシーカードシステムを展開する政府機関が使用している暫定インタフェース仕様を含む『Government Smart Card Interoperability Specification (GSC-IS)』[7] のサブセットについて記述する。

1.5.3 パート 3：最終インタフェース

パート 3 には、本文書の第 3、第 4、第 5、第 6、および第 7 節が含まれる。これらの各節では、PIV カードとクライアントアプリケーションに必須である最終インタフェースについて詳しく記述している。

+ 第 3 節「概念と構造」では、情報処理概念やデータ表現構造など、PIV クライアントアプリケーションのプログラミングインタフェースおよび PIV カードアプリケーションのコンピュータ処理モデルについて記述している。
+ 第 4 節「相互運用のためのデータオブジェクト」では、PIV クライアントアプリケーションのプログラミングインタフェースおよび PIV カードアプリケーションで使用するデータ構造の書式とコード化について記述している。
+ 第 5 節「データタイプとその表現」では、PIV クライアントアプリケーションのプログラミングインタフェースおよび PIV カードアプリケーションのカードコマンドインタフェースで使用するデータの詳細を規定している。
+ 第 6 節「PIV クライアントアプリケーションのプログラミングインタフェース」では、プログラミング言語に依存しない用語を使用して、PIV クライアントアプリケーションのプログラミングインタフェースについて記述している。
+ 第 7 節「PIV カードアプリケーションのカードコマンドインタフェース」では、PIV カードアプリケーションに対するカードコマンドインタフェースについて記述している。

1.5.4 付録

付録には、本文書の本文にある情報の理解を助けるために、図や例による資料に加えて特別な書式を必要とする資料が収録されている。

1.6 移行に関する考慮事項

本文書は、2 種類のインタフェース仕様を規定する。つまり、1) パート 2 で記述する暫定カード仕様(訳注：移行を前提としたカード仕様)と、2) パート 3 で記述する FIPS 201 PIV–II カード仕様である。パート 2 は、『Government Smart Card Interoperability Specification, Version 2.1』(NIST IR 6887) に由来する PIV のプロファイルである。このパート 2 にある PIV のプロファイルは参考情報であり、GSC-IS に基づき既にスマートカードを展開している政府機関が、パート 3 で記述するカードのデプロイメントに移行する際に採用することができる 1 つの移行パスとして提示されている。すべての政府機関は、行政管理予算局（OMB: Office of Management and Budget）が規定した計画に従って、最終的にはパート 3 仕様に適合しなければならない。したがって、パート 3 仕様の完全な展開が各政府機関の移行計画の最終到達点となる。

政府機関は、特に、現在様々な局面で実装されている ID カードアーキテクチャから、本文書の以降の節で記述するパート 3 仕様へ移行する場合に、承認済みの暫定仕様（第 2 節参照）を実装する方法を選択できるほか、パート 3 仕様を直接実装する方法も選ぶことができる。NIST は、パート 3 仕様で記述している政府全体にわたる PIV-II 相互運用性の実現に向けた政府機関の取り組みを支援する。NIST は、現在利用されている PIV デプロイメントのために、パート 3 仕様に移行するための仕様も支援する。

パート 2 の移行パスは、PIV データモデルの継続を前提としている。この移行パスに伴う特有の考慮事項を、以下に強調して列挙する。

+ パート 2 には、GSC-IS のデュアルカードエッジインタフェースのサブセットを示す。パート 3 には、既存の国際標準に適合し、テクノロジーに依存しない統一カードエッジインタフェースを示す。

+ パート 3 では、制限付きのクレデンシャル管理機能を規定する。新規カードアプリケーションのローディングを含んだ発行ドメイン間で統一され、相互運用可能なカード管理ソリューションは含まれていない。

+ データモデル内の名前付きデータオブジェクトには直接アクセスしてもかまわない。データオブジェクトがデフォルトアプリケーションによって管理される場合、アプリケーションを選択しなくてもそのデータオブジェクトを直接取得できる。そのため、名前付きデータオブジェクトを取得するためのディスカバリによる検索の必要性はなくなる。それ以外の場合は、データオブジェクトを管理する(非デフォルト)アプリケーションを選択し、そのアプリケーションからデータオブジェクトを取得する。第 6 節に記述した GET DATA コマンドは、データオブジェクトを 1 つのコマンドで取得する。

+ データモデルは、データモデルのネームスペースを含めて NIST が管理している。そのため、一般的で相互運用可能なデータオブジェクトの変更管理は、データモデル全般を管理するプロセスの中で NIST が実施することになる。ネームスペース管理の第 1 段階として、GSC-IS および暫定システムのデータオブジェクト識別子のうち'0000'から'9FFF'までの範囲にあるものは NIST が明示的に管理し、GSC-IS および暫定システムのデータオブジェクト識別子のうち'A000'から'FFFF'までの範囲にあるものは、カード発行者の管理下に置く。

+ 直接処理可能なデータモデルデータオブジェクトを 1 つ以上管理している各アプリケーションは、データオブジェクトが依存するアプリケーションがオブジェクト内に含まれている情報レベルを判別できるように、バージョン番号を持っている。パート 3 の PIV カードアプリケーションのバージョンは、完全なアプリケーション識別子(AID)内で符号化されている。この AID は、アプリケーションが選択された際に返される。これは、GSC-IS から引き継がれるカード機能コンテナ(CCC)方式のデータモデル命名機構に追加されるものである。

+ PIV アプリケーションを含むカードには、政府機関固有のアプリケーションを組み込むことができる。こういったアプリケーションでは、アプリケーション使用時に利用する独自のネームスペースを定義し、管理することができる。このアプリケーションは、NIST が管理しているアプリケーションネームスペースの範囲外のアプリケーション識別子、つまり、NIST 登録済みアプリケーション提供者識別子(RID)を起源としないアプリケーション識別子を持つ。

1.7 PIV データモデル

SP 800-73 での PIV データモデルは、GSC-IS 仕様に従って構成されている。表 1 は、データモデルをハイレベルな視点で定義したものである。各コンテナは、「必須」または「オプション」のいずれかにラベル付けされている。必須データ要素は、パート 2 とパート 3 の双方に共通である。このデータモデルは、デュアルインタフェースカードをサポートできるように設計されている。インタフェースモード(接触/非接触)に基づくアクセス条件は、表 1 の第 3 欄に定義されているアクセス規則より優先されることに注意する必要がある。

付録 A には、データモデルの詳細なスプレッドシートを用意した。コンテナ内のコンテナ ID およびタグは、本データモデルによって、また SP 800-73 命名規則に従って定義されている。フィールドの長さやバッファのサイズについてはガイダンスを示している。これらの長さやサイズは、オプションのコンテナと同様に、カード発行者の管理下に置く。カード発行者は、実装固有のニーズに応じて、具体的なデータサイズ要件を算出すべきである。

-

表 1. SP 800-73 データモデルのコンテナ

RID 'A0 00 00 00 01 16'	コンテナ ID	アクセス規則	接触／非接触	必須／オプション
カード機能コンテナ	0xDB00	常に読み込み	接触	必須
CHUID バッファ	0x3000	常に読み込み	接触および非接触	必須
PIV 認証の証明書バッファ	0x0101	常に読み込み	接触	必須
指紋バッファ	0x6010	PIN	接触	必須
印刷情報バッファ	0x3001	PIN	接触	オプション
顔画像バッファ	0x6030	PIN	接触	オプション
ディジタル署名の証明書バッファ	0x0100	常に読み込み	接触	オプション
鍵管理の証明書バッファ	0x0102	常に読み込み	接触	オプション
カード認証の証明書バッファ	0x0500	常に読み込み	接触	オプション
セキュリティオブジェクトバッファ	0x9000	常に読み込み	接触	必須

1.8 必須データ要素

必須データコンテナは、FIPS 201 で最低限必要となる適合性をサポートする。

1.8.1 カード機能コンテナ（Card Capability Container:CCC）

CCC は、GSC-IS 仕様に適合する上で必須である。これは、データモデルおよびアプリケーション情報の検索について最小限の機能をサポートする。

データモデルは、データモデル番号 '0x10' によって識別しなければならない。展開されるアプリケーションでは、'0x00' から '0x04' を使用する。これによって、GSC-IS アプリケーションドメインが、本文書で定義されている新たなデータモデルのネームスペースおよび構造を正確に識別することができるようになる。

1.8.2 PIV 認証鍵

個人識別番号（PIN）を使用してカードおよびカード所有者を識別する際には、FIPS 201 で定義されている PIV 認証鍵を使用する。

1.8.3 CHUID

カード所有者のユニークな識別子（CHUID）バッファは、『技術実装ガイダンス：Smart Card Enabled Physical Access Control Systems (TIG SCEPACS)』[5] に従って定義されている。この仕様では、CHUID は接触型チップと非接触型チップで共通である。デュアルチップ実装の場合は、2 つのチップ間で CHUID がそのままコピーされる。

PIV カード上の CHUID は、TIG SCEPACS で規定されている要件に加えて、以下の要件を満たさなければならない。

+ 9,999,999,999 個のクレデンシャルに対するクレデンシャル番号スペースを確立するためには、Federal Agency Smart Credential Number (FASC-N) が「System Code || Credential Number」について TIG SCEPACS Option と一致していなければならない。
+ グローバルでユニークな識別子（GUID）フィールドが存在しなければならない。このフィールドは、発行者が割り付けた IPv6 アドレスを含むか、すべてゼロとしてコーディングされる。GUID は、発行されたすべてのクレデンシャルに対して FASC-N から堅牢な番号付けスキームへ将来移行できるようにするために含まれている。
+ DUNS および組織コードフィールドはオプションである。
+ 認証鍵マップは、アプリケーションが鍵参照を発見できるようにするためのオプションフィールドとして規定されている。これは、カード認証鍵を使用した、対象型チャレンジレスポンスプロトコルを実装するひとつの方法である。
+ Expiration Date は Reserved for Future Use (RFU) タグ 0x35 にマップされ、それを TIG SCEPACS 仕様の従来の範囲内に維持している。このフィールドは 8 バイト長で、YYYYMMDD 形式でコード化しなければならない。
+ CHUID は FIPS 201 に従って署名される。CHUID に署名するには、カード発行者のディジタル署名鍵を使用しなければならない。CHUID の署名フィールドには、カード発行者の証明書が含まれる。

1.8.4 指紋

指紋バッファは、FIPS 201 に従って 1 次指紋および 2 次指紋を指定する。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（CBEFF）ヘッダーは、FASC-N を含まなければならず、完全性オプションを必要とする。このヘッダーは、機密性オプションを必要としない。

1.8.5 セキュリティオブジェクト

セキュリティオブジェクトは、『PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1』[8] の付録 C に従う。Machine Readable Travel Document (MRTD) で規定される 16 個のデータグループに PIV データモデルのコンテナ ID をマップするには、タグ '0xBA' を使用する。これによって、セキュリティオブジェクトが識別情報文書に関する将来の活動に完全に適合することができるようになる。

CHUID の署名に用いられるカード発行者のディジタル署名鍵を、セキュリティオブジェクトの署名にも使用しなければならない。発行者の証明書は CHUID に含まれているので、セキュリティオブジェクトの署名フィールドから発行者の証明書を除外しなければならない。

1.9 オプションのデータ要素

FIPS 201 のオプションのデータ要素を実装する場合は、本文書で規定する仕様に適合しなければならない。

1.9.1 印刷情報バッファ

カード上に印刷される FIPS 201 のすべての必須情報は、このバッファ内でチップ上に複写される。セキュリティオブジェクトは、発行者によりこの情報の完全性を確保する。（訳注:「発行者が複写することにより…完全性の確保を強化する。」の意味を含んでいる）。これは、カード情報が印刷情報と一致しなければならないという具体的な保護手段を提供し、印刷媒体での改ざんのリスクを低減する。

1.9.2 顔画像バッファ

チップ上の写真は、人間による検証のみをサポートする。自動的に本人を確認する顔認識システムをサポートすることは意図していない。セキュリティオブジェクトは、発行者によりこの情報の完全性を確保する。(訳注:「発行者が複写することにより…完全性の確保を強化する。」の意味を含んでいる)。これは、カード情報が印刷情報と一致しなければならないといった具体的な保護手段を提供し、印刷媒体での改ざんのリスクを低減する。

1.9.3 ディジタル署名鍵

この鍵と証明書は、文書に署名するためのディジタル署名の使用をサポートする。公開鍵インフラストラクチャ(PKI)暗号機能は、「常に PIN」というアクセス規則によって保護される。これには、鍵を使用してディジタル署名を生成するたびに、カード所有者が関与する必要がある。

1.9.4 鍵管理鍵

この鍵と証明書は、機密性を目的とする暗号化の使用をサポートする。この鍵ペアは、鍵復元のために発行者がエスクローする。PKI 暗号機能は、「PIN」アクセス規則によって保護される。これにはカード所有者による活性化が必要であるが、カード所有者の更なる同意がなくても、複数の計算操作が可能になる。

1.9.5 カード認証鍵

鍵が非対称であった場合、この鍵と証明書はデバイス間の認証を実施するために必要な PIV カード認証をサポートする。この鍵を使用するのに、カード所有者の同意は必要ない。PKI 暗号機能のアクセス規則は「常に(always)」である。カード認証鍵が対称鍵の場合、暗号アルゴリズムと鍵の格納場所を指定する CHUID 認証鍵マップが存在しなければならない。

2. パート 2:移行カードインタフェース

2.1 PIV アプリケーションプログラミングインタフェース

2.1.1 基本サービスインタフェース

本章は、PIV アプリケーションに提供される基本サービスインタフェース(BSI)サービスを定義する。以下の仕様は、特に断りがない限り NIST Interagency Report (NISTIR) 6887 に適合している。

以下に示す関数は、NISTIR 6887 のサブセットである。本書で定義する PIV アプリケーションのユースケースを実装するには、これらの関数が必要である。

+ gscBsiUtilAcquireContext ()
+ gscBsiUtilConnect ()
+ gscBsiUtilDisconnect ()
+ gscBsiUtilBeginTransaction ()
+ gscBsiUtilEndTransaction ()
+ gscBsiUtilGetVersion ()
+ gscBsiUtilGetCardStatus ()
+ gscBsiUtilGetExtendedErrorText ()
+ gscBsiUtilGetReaderList ()
+ gscBsiUtilReleaseContext ()
+ gscBsiGcReadTagList ()
+ gscBsiGcReadValue ()
+ gscBsiPkiCompute ()

2.2 PIV カードアプリケーションバージョン

接触モードと非接触モードのいずれの場合も、CHUID をホストするアプリケーションが PIV カード上に常に必要となる。アプリケーションが選択された時には、選択に対する応答として、そのアプリケーションは PIV アプリケーションバージョンを返さなければならない。

PIV アプリケーションバージョンは以下の情報を示す。

1. サポートされるカードエッジ仕様へのリファレンス
2. PIV データモデルオブジェクト識別子

3. 必須アプリケーションとそれらの AID のリスト

4. アプリケーションごとの PIV データモデルの必須サブセットへのリファレンス(オブジェクト識別子)

5. アプリケーションごとの暗号機能

接触モードと非接触モードのいずれについても特定の値が規定されている。

接触モードと非接触モードのいずれの場合も、カード上の CHUID を含む PIV アプリケーションに対する SELECT への応答として、PIV アプリケーションバージョンが返される。

返されるアプリケーション名の最終バイトは、カード内のアプリケーションバージョンと、仮想マシン(VM)またはファイルシステム(FS)のカードタイプを示す。

カードによって返されるアプリケーションバージョンのバイトは、以下のように構成されている。

Bit8 = 0b VM カードエッジ

Bit8 =1b FS カードエッジ

Bits 7-1 このカード内の PIV アプリケーションバージョン
この番号は、PIV カードが準拠する SP800-73 仕様のリリースを示す。

表 2. 完全な PIV カードのバージョン

PIV アプリケーション バージョン	記述	データモデル
0x00	VM カード上の完全な PIV	PIV データモデルオブジェクト識別子
0x80	sFS カード上の完全な PIV	PIV データモデルオブジェクト識別子

2.2.1 PIV オブジェクトの命名構造

+ カードエッジレベルでは、オブジェクトは GSC-IS オブジェクト識別子(2 バイト)によって参照され、AID 内に置かれる。この場合、AID = 発行者 RID(5 バイト)|| PIX となる。これに関連して、Proprietary Identifier eXtension (PIX) は 2 バイトからなる:アプリケーション ID

+ CCC 内にリストされている各カードアプリケーションの Uniform Resource Locator (URL) は、以下の順番に並ぶ要素で構成される。

  - 発行者 RID(カード発行者に割り付けられる任意の値)。

  - カードアプリケーションタイプ:PKI、GC:これは、オブジェクトに対して使用可能なアプリケーションプロトコルデータ単位(APDU)コマンドを示す。

  - GSC-IS オブジェクト識別子。選択するコンテナまたはオブジェクトを識別する。

  - AID または PIX。

以下の CardApplicationURL フィールド（AccessProfile、pinID、AccessKeyInfo、keyCryptoAlgorithm）はいずれも、VM カードに関する PIV アプリケーションの場合は存在しないが、ファイルシステムカードについてはオプションのフィールドである。

+ BSI レベルでは、オブジェクトは 7 バイトの GSC-IS オブジェクト AID（発行者 RID || GSC-IS オブジェクト識別子）によって参照される。

+ ドアリーダで、または PIV アプリケーションからカードエッジに直接アクセスする場合、オブジェクトは 2 バイトの GSC-IS オブジェクト識別子によって参照される。

2.2.2 マッピングメカニズム

CCC CardApplicationURL は、GSC-IS オブジェクト識別子を検索し、選択に利用される対応アプリケーション識別子を構成するのに使用する。

2.3 カードエッジコマンド

2.3.1 一般

PIV アプリケーションは、相互運用性を確保し、GSC-IS をベースとする既存システムとの互換性を維持するために、VM およびファイルシステムのデュアルカードエッジをサポートする。

PIV アプリケーションには、非接触インタフェースも必要である。非接触コマンドインタフェースは、NISTIR 6887 の「付録 G」に適合している。ただし、仮想マシンとファイルシステムのいずれの場合も、非接触インタフェースは「付録 G」で定義されているオブジェクト ID やタグではなく、本 800-73 仕様書で定義するデータモデルのオブジェクト ID やタグに依存している。デュアルインタフェースの VM カードには、カードがリセットに応答した直後に発行される Select Object/EF CHUID を VM カードが受け取れるように、デフォルトで選択されたアプレットの中に選択可能な CHUID オブジェクトが存在しなければならない。

インタフェースに提示される情報は、NISTIR 6887 に記述されているようなカードエッジタイプ固有の書式を持つ。

2.3.2 データの書式と構造

NISTIR 6887 の第 8.2、第 8.3、第 8.4 節を参照。

2.3.3 PIV カードエッジコマンド

PIV の要件を満たすには、GSC-IS コマンドのサブセットだけが必要である。APDU は、2 つのカテゴリに分かれている。すなわち、共通インタフェース用コマンドと認証用コマンドである。

注：PIV カードは、VM カードエッジまたは FS カードエッジのいずれかをサポートしなければならない。カードエッジ間で異なる APDU を組み合わせることは許容されていない。

ADPU コマンドおよび応答は、NISTIR 6887 の表 5-2 および表 5-3 で定義されている。

VM カードコマンドを使用して PIV カードを実装するには、以下のカードコマンドが必要である。

表 3. VM カードコマンド

タイプ	コマンド名
共通インタフェース用コマンド	SELECT APPLET / SELECT OBJECT
	GET RESPONSE
共通インタフェース用カードプラットフォームコマンド	READ BUFFER
認証用コマンド	VERIFY
	PRIVATE SIGN / DECRYPT

使用可能なコマンドセットは、その時点で選択されているオブジェクトによって異なることに注意されたい。

+ コンテナオブジェクトの選択後は、PRIVATE SIGN/DECRYPT を除く上記のすべてのコマンドが使用可能になる。
+ PKI オブジェクトの選択後は、上記のすべてのコマンドが使用可能になる。

ファイルシステムカードコマンドを使用して PIV カードを実装するには、以下のカードコマンドが必要である。

表 4. ファイルカードコマンド

タイプ	コマンド名
共通インタフェース用コマンド	SELECT
	GET RESPONSE
共通インタフェース用カードプラットフォームコマンド	READ BINARY
認証用コマンド	VERIFY
	MANAGE SECURITY ENVIRONMENT
	PERFORM SECURITY OPERATION

2.3.3.1 共通インタフェース用の VM カードプラットフォームコマンド

2.3.3.1.1 SELECT APPLET/SELECT OBJECT APDU

SELECT コマンドには、VM カードで 1) 現在選択されているアプリケーションを設定する、2) 現在選択されているオブジェクトを設定する、という 2 つの目的がある。

コマンドメッセージ

CLA	0x00
INS	0xA4
P1	リファレンス制御パラメタ
P2	0x00
Lc	データフィールドの長さ
Data Field	アプレット AID またはカードオブジェクト ID
Le	空

リファレンス制御パラメタ P1

パラメタ P1 は、実行する選択のタイプを示す。指定できる値は次のとおりである。

- 04h:AID によるアプリケーションの選択、および結果としての本アプリケーションでのデフォルトオブジェクトの選択
- 02h:オブジェクト識別子によるオブジェクトの選択。
- 本コマンドは、AID またはファイル ID を使用したオブジェクトの選択をサポートする。

コマンドメッセージで送信されるデータフィールド

アプリケーション選択の場合、データフィールドには AID が格納される。

オブジェクト選択の場合、データフィールドにはオブジェクト識別子が格納される。

応答メッセージ

応答メッセージで返されるデータフィールド

APDU の結果が成功を示している場合、

カードオブジェクト選択の場合、応答メッセージはステータスワード(SW)を除いて NULL である。

NISTIR 6887 に対する追加:アプレット選択の場合、応答メッセージには、ISO-7816-4 (FCI) で定義される最小限のファイル制御情報が以下のように格納される。

オフセット	値	記述
00h	6Fh	FCI テンプレートタグ
01h	4 + AID の長さ	FCI テンプレートの長さ
02h	84h	アプリケーション名タグ
03h	AID の長さ	アプリケーション名の長さ
04h	AID	インスタンス AID 値
4+ AID の長さ	A5h	個別に定義されたデータタグ
5+ AID の長さ	00h	Length=00

応答メッセージで返される処理状態

SW1	SW2	意味
6A	82	アプリケーションが見つからない
90	00	正常実行
69	99	選択に失敗(カードプラットフォームが返す)ー NISTIR 6887 に対する追加

2.3.3.1.2 GET RESPONSE APDU

NISTIR 6887 の第 5.3.3.6 節を参照。

2.3.3.1.3 READ BUFFER APDU

NISTIR 6887 の第 5.3.4.2 節を参照。

2.3.3.2 認証用 VM カードプラットフォームコマンド

2.3.3.2.1 VERIFY APDU

本 APDU は、PIN をスマートカード上の対応する認証データと比較するために使用する。ホストは認証データを本 APDU に入れて送信し、スマートカードに対してスマートカード上の認証データと比較するように指示する。認証データは暗号化せずに渡される。

コマンドメッセージ

CLA	0x00
INS	0x20
P1	0x00
P2	0x00
Lc	データフィールドの長さ。8 でなければならない。
データフィールド	認証データ（つまり、PIN）
Le	空

注：Lc=0x00、かつコマンドのデータフィールドが空であれば、本コマンドを使用して、今後許容されるリトライ回数を取得できるほか、検証が必要ないかどうかをチェックできる。

鍵リファレンス識別子 P2

ファイルカードエッジを利用する PIV カードで使用する PIN は、NISTR 6887 のほかに第 3.5.3 節で定義する PIN 書式に適合しなければならない。

応答メッセージ

応答メッセージで返されるデータフィールド

空。

応答メッセージで返される処理状態

SW1	SW2	意味
63	00	検証に失敗した。
63	CX	検証に失敗した。X は、今後許容されるリトライの数を示す。
69	83	認証処理がブロックされた。
69	84	参照されているデータが非活性化されている。
6A	86	パラメタ P1-P2 が正しくない。
6A	88	リファレンスデータが見つからない。
90	00	正常実行。

2.3.3.2.2 PRIVATE SIGN/DECRYPT APDU

本コマンドは、Rivest、Shamir、Aldeman (RSA) 署名またはデータ復号化を実行するために使用する。

コマンドメッセージ

CLA	0x80
INS	0x42
P1	リファレンス制御パラメタ P1
P2	0x00
Lc	データフィールドの長さ
データフィールド	署名または復号化するデータ
Le	予想される署名／復号化の長さ

リファレンス制御パラメタ P1 (NISTIR 6887 に対する追加)

制御パラメタ P1 は、データを含むブロックがさらに続いているかどうかを示す。本パラメタは、2048 ビット以上の RSA 操作用に入力データを輸送するために、複数の APDU を連結するのに使用する。本コマンド連鎖方式は、IC に関する国際標準である ISO/IEC 7816、 Information Technology – Identification Cards – Integrated Circuit(s) Card with Contacts [1] に適合していないため、ICC の国際標準に適合しているパート 3 のコマンド連結方式との互換性もない点に注意されたい。

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	X	X	X	X	X	X	X	後続のブロックはこれ以上存在しない
1	X	X	X	X	X	X	X	後続のブロックがさらに存在する

コマンドメッセージで送信されるデータフィールド

データフィールドには、選択された RSA 鍵ペアを使用して署名されるデータが格納される。

本データは、メッセージを送信する前に埋め込んでおかなければならない。

応答メッセージ

応答メッセージで返されるデータフィールド

応答メッセージ内のデータフィールドには、署名または復号化されたデータが格納される。データ埋め込みは、すべてクライアントアプリケーションの責任で行う。

応答メッセージによって返される処理状態

SW1	SW2	意味
67	00	コマンドデータの長さが RSA 鍵サイズと等しくない。
69	83	RSA プライベート鍵が初期設定されていない。
69	82	アクセス条件を満たしていない。

69	85	使用条件を満たしていない（現在選択されているオブジェクトが無効）。
61	XX	正常処理の場合、XX バイトのデータが読み込まれ、その後の Get Response で利用可能になる。

2.3.3.3 ファイルカードプラットフォームコマンド

2.3.3.3.1 SELECT APDU

NISTIR 6887 の第 5.1.1.3、第 5.1.1.3.1、第 5.1.1.4、および第 5.1.1.5 節を参照。暫定 PIV アプリケーションに必要な SELECT コマンドは 2 つのみである。「Select EF」をサポートする必要がある（P1=0x00 または P1=0x02）ほか、CCC にアクセスするためにすべてのカードで「Select File by name」を使用する必要がある。これは、別のメカニズムを使用してカード上で使用可能なカードエッジを調べる GSC-IS とは異なるものである。

注：GSC-IS では、ファイルカードで APDU コマンドの「Select DF by name」がサポートされている場合でも、CCC はそれがファイルカードであることを調べられるようにする CCC の名前として GSA AID (A00000000116DB00)を使用してはならない。これが本仕様での相違点である。

2.3.3.3.2 GET RESPONSE APDU

NISTIR 6887 の第 5.1.1 節を参照。

2.3.3.3.3 READ BINARY APDU

NISTIR 6887 の第 5.1.1 節を参照。

2.3.3.3.4 MANAGE SECURITY ENVIRONMENT

NISTIR 6887 の第 5.1.3.1 節を参照。

2.3.3.3.5 PERFORM SECURITY OPERATION APDU

NISTIR 6887 の第 5.1.1 節を参照。

2.3.3.3.6 VERIFY APDU

NISTIR 6887 の第 5.1.1 節を参照。

ファイルカードエッジを利用する PIV カードで使用する PIN は、NISTR 6887 のほかに第 3.5.3 節で定義する PIN 書式に適合しなければならない。

2.4 一般的なステータス条件

一般的なステータス条件については NISTIR 6887 を参照。

3. パート 3:最終インタフェースの概念と構造

Special Publication 800-73 パート 3 は、個人識別情報検証(PIV)カードアプリケーションを含む ICC への 2 つのインタフェースを定義している。つまり、上位レベルの PIV クライアント API と、下位レベルの PIV カードアプリケーションカードコマンドインタフェース(カードエッジ)である。

いずれのインタフェースでも情報処理の概念やデータ構造は同じであり、クライアントアプリケーションプログラミングインタフェースやカードコマンドインタフェースについては特に言及せず、一般に *PIV インタフェース*での情報処理の概念やデータ構造と呼ぶ場合もある。

クライアントアプリケーションプログラミングインタフェースは、これらの概念や構造に対してタスク固有のプログラムアクセスを提供し、カードコマンドインタフェースは、これらの概念や構造に対して通信アクセスを提供する。クライアントアプリケーションプログラミングインタフェースは、PIV カードアプリケーションを使用するクライアントアプリケーションで使用する。カードコマンドインタフェースは、クライアントアプリケーションプログラミングインタフェース(ミドルウェア)を実装するソフトウェアで使用する。

クライアントアプリケーションプログラミングインタフェース上の単一の入口点へのアクセスによって、複数のカードコマンドがカードコマンドインタフェースを行き来する場合があるので、クライアントアプリケーションプログラミングインタフェースの方がカードコマンドインタフェースよりも上位レベルであると考えられる。つまり、クライアントアプリケーションプログラミングインタフェース上の入口点での 1 回の呼び出しで表されるタスクを遂行するために、カードコマンドインタフェース上では複数のカードコマンドを必要とする場合がある。

クライアントアプリケーションプログラミングインタフェースがプログラム実行、呼び出し／戻り型のインタフェースであるのに対して、カードコマンドインタフェースは通信プロトコルのコマンド/応答型インタフェースである。この相違があるため、PIV の概念や構造をクライアントアプリケーションプログラミングインタフェース上でビット形式やバイト形式で表現した場合と、同じ概念や構造をカードコマンドインタフェース上で表現した場合とでは異なることがある。

3.1 統一されたカードコマンドインタフェース

PIV カードアプリケーションのカードコマンドインタフェースは、GSC-IS および上述の第 2 節の 2 種類のカードコマンドインタフェースを統一したものである。

この統一は、GSC-IS 仮想マシンカードエッジのコンピュータ処理についてオブジェクト指向モデルを採用し、GSC-IS ファイルシステムカードエッジの基盤となる ICC の国際標準 [1] にあるデータ構造や操作を使用してその技術的な詳細を実現することによって、達成されている。そのため、PIV カードアプリケーションは、GSC-IS の既存の展開への影響を最小限にとどめながら、この標準への適合性を実現している。

この統一の結果、PIV カードアプリケーションと、それにアクセスするクライアントアプリケーションのふるまいは、PIV カードアプリケーションが導入される ICC プラットフォームに依存しないものになっている。

3.1.1 プラットフォームの要件

PIV カードアプリケーションを実装する ICC プラットフォームには、次の要件が課される。

- グローバルなカード所有者の PIN のセキュリティステータスを含めた、グローバルセキュリティステータス
- 短縮 AID を使用したアプリケーション選択
- 個々のアプリケーションのセキュリティステータスをリセットする機能
- 接触型と非接触型のどちらの物理通信インタフェースが使用されているかを、アプリケーションに通知
- ウォームリセットまたはコールドリセット時における、アプリケーションのデフォルト選択のサポート

3.2 PIV カードアプリケーションのネームスペース

PIV インタフェースで使用される名前は、NIST が管理する次の 3 つのネームスペースに由来している。

- NIST RID の PIX
- NIST が管理する OID の個人検証サブセットにある ASN. 1 オブジェクト識別子（OID）
- 基本コード化規則 – NIST PIV 共存タグ割り当てスキームの Tag Length Value (BER-TLV) タグ

これらの管理されたネームスペースに含まれている未規定の名前は、すべて将来の使用のために予約されている。

[1] で定義され、再定義なしに NIST 共存タグ割り当てスキームで使用されているすべての産業間タグは、NIST PIV 共存タグ割り当てスキームでも [1] と同じ意味を持つ。

次の識別子および値ネームスペースにある未規定の名前は、すべて将来の使用のために予約されている。

- アルゴリズム識別子
- 鍵リファレンス値
- 暗号メカニズム識別子

3.3 データオブジェクト

*データオブジェクト*は、カードコマンドインタフェース上で見られる情報項目で、名前、論理的な内容の記述、書式、およびコード化が規定されている。各データオブジェクトは、ISO/IEC 8824-2:2002, Information technology – Abstract Syntax Notation One (ASN. 1): Information object specification [2] で定義されている、*オブジェクト識別子*と呼ばれるグローバルにユニークな名前を持つ。

データ内容が、ISO/IEC 8825-1:2002, Information technology – ASN. 1 encoding rules [3] にあるような BER-TLV データ構造としてコード化されているデータオブジェクトは、*BER-TLV データオブジェクト*と呼ばれる。

3.3.1 データオブジェクトの内容

データオブジェクトの*内容*とは、データオブジェクトに*含まれる*、またはデータオブジェクトの*値*と言われるバイト列のことである。このバイト列のバイト数は、データ内容の*長さ*と呼ばれるほか、データオブジェクトの*サイズ*とも呼ばれる。バイト列の先頭バイトは、データオブジェクトの内容の*バイト位置* 0 または*オフセット* 0 であると見なされる。

BER-TLV データオブジェクトのデータ内容は、他の BER-TLV データオブジェクトから構成されている場合がある。この場合、データオブジェクトのタグは、それが複数の BER-TLV データオブジェクトで*構成されたデータオブジェクト*であることを示す。複数の BER-TLV データオブジェクトにより構成されていない BER-TLV データオブジェクトは、*基本データオブジェクト*と呼ばれる。

3.4 カードアプリケーション

カードコマンドインタフェースに現れる各コマンドは、ICC 内に常駐する*カードアプリケーション*によって実装しなければならない。カードコマンドは、カードアプリケーションがアクセスするデータオブジェクトに対する操作や、それらのデータオブジェクトを使用した操作を実行できるようにする。

それぞれのカードアプリケーションは、アプリケーション識別子（AID）と呼ばれるグローバルでユニークな名前を持たなければならない [1、パート 4] 。カードコマンドやカードアプリケーションのデータオブジェクトへのアクセスは、そのアプリケーション識別子を使用してカードアプリケーションを選択することによって行わなければならない。AID の PIX には、カードアプリケーションのバージョンをコード化した情報を格納しなければならない。

あるカードアプリケーションのカードコマンドが現在使用されている場合、そのカードアプリケーションを*現在選択されているアプリケーション*と呼ぶ。

3.4.1 個人識別情報検証カードアプリケーション

個人識別情報検証カードアプリケーション（PIV カードアプリケーション）には、以下の AID を割り当てなければならない。

'A0 00 00 03 08 00 00 10 00 01 00'

PIV カードアプリケーションの AID は、NIST RID (‘A0 00 00 03 08’) と、それに続く PIV カードアプリケーションを示す NIST PIX のアプリケーション部分 (’00 00 10 00’)、および PIV カードアプリケーションの最初のバージョンを示す NIST PIX のバージョン部分 (’01 00’) で構成されている。PIV カードアプリケーション AID の末尾 5 バイトを含む、NIST RID の他のすべての PIX シーケンスは、将来の使用のために予約されている。

PIV カードアプリケーションは、第 7 節に記述するカードコマンドをカードコマンドインタフェース上に表す。

3.4.2 デフォルトで選択されるカードアプリケーション

カードプラットフォームは、デフォルトで選択されるカードアプリケーションをサポートしなければならない。言い換えれば、コールドリセットまたはウォームリセットの直後に、現在選択されているアプリケーショ

ンが存在しなければならない。このカードアプリケーションが、デフォルトで選択されるカードアプリケーションである。

PIV カードアプリケーションは短縮形式の AID によって選択できるので、選択されるカードアプリケーションは、PIV カードアプリケーションである場合と、別のカードアプリケーションである場合がある。

3.5 セキュリティアーキテクチャ

ICC のセキュリティアーキテクチャは、カード上に格納されている各データオブジェクトへのアクセスを管理するセキュリティ方針をカード内で表現するための手段である。

ICC 内のソフトウェアは、このセキュリティ方針表現をあらゆるカードコマンドに適用することによって、カードアプリケーションに対する所定のデータ方針が確実に実施されるようにする。

以下のサブセクションでは、PIV カードアプリケーションのセキュリティアーキテクチャについて記述する。

3.5.1 アクセス制御規則

*アクセス制御規則*は、*アクセスモード*と*セキュリティ条件*から構成されていなければならない。アクセスモードとは、データオブジェクトに対して実行可能な操作である。セキュリティ条件とは、以下に定義するセキュリティステータスと呼ばれる変数を使用したブール表現である。

アクセス制御規則によれば、アクセスモードによって記述されるアクションがデータオブジェクトに対して実行できるのは、セキュリティステータスの現在の値に対するセキュリティ条件の評価が TRUE である場合のみである。特定のアクションを記述するアクセスモードのアクセス制御規則がない場合は、このアクションをデータオブジェクトに対して実行してはならない。

3.5.2 セキュリティステータス

それぞれの認証可能エンティティに関連して、認証可能エンティティの*セキュリティステータス標識*と呼ばれる 1 つ以上のブール変数のセットがなければならない。認証可能エンティティのセキュリティステータス標識は、そのセキュリティステータス標識に関連付けられているクレデンシャルが既に認証されている場合は TRUE になり、それ以外の場合は FALSE にならなければならない。

認証プロトコルが正常に実行されると、そのプロトコルによって検証されたクレデンシャルに関連付けられたセキュリティステータス標識を TRUE に設定しなければならない。

例えば、カード所有者の 3 つのセキュリティステータス標識に関連付けられたクレデンシャルが、PIN、指紋、および音声バイオメトリックとなる可能性がある。第 1 のセキュリティステータス標識に対する認証プロトコルは、PIN の知識を実証することである。カード上の指紋テンプレートをカード所有者から入手した指紋と比較することが、第 2 のセキュリティステータス標識に対する認証プロトコルである。音声サンプルを入手し、音声テンプレートと比較することが、第 3 のセキュリティステータス標識に対する認証プロトコルである。この 3 つのセキュリティステータス標識を使用したセキュリティ条件は、(PIN AND 指紋) OR(音声バイオメトリック))となるかもしれない。

現在選択されているアプリケーションが、あるアプリケーションから別のアプリケーションに変わってもセキュリティステータス標識が変化しない場合、このセキュリティステータス標識を*グローバル*セキュリティステータス標識と呼ぶものとする。

現在選択されているアプリケーションが、あるアプリケーションから別のアプリケーションに変更されるとセキュリティステータス標識が FALSE に設定される場合、このセキュリティステータス標識を*アプリケーション*セキュリティステータス標識と呼ぶ。あらゆるセキュリティステータス標識は、グローバルセキュリティステータス標識かアプリケーションセキュリティステータス標識のいずれかである。

*グローバルセキュリティステータス*という用語は、グローバルセキュリティステータス標識すべてのセットを指す。*アプリケーションセキュリティステータス*という用語は、特定のアプリケーションに関するアプリケーションセキュリティステータス標識すべてのセットを指す。

3.5.3 個人の認証

PIN の知識は、PIV カードアプリケーションに対して個人を認証する手段のひとつである。

カードコマンドインタフェースに渡す個人識別番号（PIN）は 8 バイト長でなければならない。実際の PIN の長さが 8 バイト未満である場合は、'FF'を埋め込んで 8 バイトにしなければならない。'FF' の埋め込みバイトは、実際の PIN の末尾に付加しなければならない。PIN を構成するバイトに 'FF' が含まれていてはならない。例えば、

- 実際の PIN:"123456"つまり'31 32 33 34 35 36'
- カードコマンドインタフェースに渡す埋め込み後の PIN:'31 32 33 34 35 36 FF FF'

3.6 PIV カードアプリケーションの現在の状態

PIV カードアプリケーションが現在選択されているアプリケーションである場合、PIV カードアプリケーションの*現在の状態*の要素は表 5 に記述するとおりである。

表 5. PIV カードアプリケーションの状態

状態名	常に定義	コメント	状態のロケーション
グローバルセキュリティステータス	Yes	プラットフォーム上のすべてのカードアプリケーションにわたるセキュリティステータス標識を含む。	PIV プラットフォーム
現在選択されているアプリケーション	Yes	プラットフォームは、右側を切り捨てたアプリケーション識別子によるカードアプリケーションの選択をサポートしなければならない。また、現在選択されているアプリケーションが常に存在しなければならない。	PIV プラットフォーム
アプリケーションセキュリティステータス	Y es	PIV カードアプリケーションに対してローカルなセキュリティステータス標識を含む。	PIV カードアプリケーション

4. パート 3:最終インタフェースでのデータオブジェクト

4.1 PIV カードアプリケーションのデータオブジェクト

PIV カードアプリケーションには、相互運用のために 6 種類の必須データオブジェクトと 5 種類のオプションのデータオブジェクトを含まなければならない。相互運用のための 6 種類の必須データオブジェクトは次のとおりである。

1. カード機能コンテナ
2. カード所有者のユニークな識別子
3. PIV 認証に対する X.509 証明書
4. カード所有者指紋 I
5. カード所有者指紋 II
6. セキュリティオブジェクト

相互運用のための 5 種類のオプションのデータオブジェクトは次のとおりである。

1. カード所有者顔画像
2. 印刷された情報
3. PIV ディジタル署名に対する X.509 証明書
4. PIV 鍵管理に対する X.509 証明書
5. カード認証に対する X.509 証明書

4.2 PIV カードアプリケーションデータオブジェクトの OID およびタグ

表 6 は、相互運用のための 11 種類の PIV カードアプリケーションデータオブジェクトについて、ASN.1 オブジェクト識別子(OID)と BER-TLV タグをリストしたものである。PIV カードアプリケーションの CCC 内で、CardApplicationURL に PIV カードアプリケーションデータオブジェクト名を構成するには、NIST RID ('A0 00 00 03 08') を使用し、カードアプリケーションタイプを '00' に設定しなければならない。3 バイトから成る BER-TLV タグの最後のバイトは、セキュリティオブジェクトを構成するためのコンテナ ID に相当する。表 1 は、相互運用のための 11 種類の PIV カードアプリケーションデータオブジェクトのアクセス制御規則をリストしたものである。これらの認証可能エンティティに関連づけられる鍵参照とアルゴリズムについては、表 12 を参照されたい。

表 6. 相互運用のための PIV データオブジェクトのオブジェクト識別子

相互運用のためのデータオブジェクト	ASN.1 OID	BER-TLV タグ	必須(M)／オプション(O)
カード機能コンテナ	2.16.840.1.101.3.7.1.219.0	'5FC107'	M
カード所有者のユニークな識別子	2.16.840.1.101.3.7.2.48.0	'5FC102'	M

PIV 認証に対する X.509 証明書	2.16.840.1.101.3.7.2.1.1	‘5FC105’	M
カード所有者指紋	2.16.840.1.101.3.7.2.96.16	‘5FC103’	M
印刷された情報	2.16.840.1.101.3.7.2.48.1	‘5FC1 09’	O
カード所有者顔画像	2.16.840.1.101.3.7.2.96.48	‘5FC108’	O
ディジタル署名に対する X.509 証明書	2.16.840.1.101.3.7.2.1.0	‘5FC10A’	O
鍵管理に対する X.509 証明書	2.16.840.1.101.3.7.2.1.2	‘5FC10B’	O
カード認証に対する X.509 証明書	2.16.840.1.101.3.7.2.5.0	‘5FC101’	O
セキュリティオブジェクト	2.16.840.1.101.3.7.2.144.0	‘5FC106’	M

5. パート 3:最終インタフェースでのデータタイプとその表現

本節では、PIV クライアントアプリケーションプログラミングインタフェースと PIV カードアプリケーションコマンドインタフェースで使用する各データタイプについて記述する。特に指示がない限り、表現はいずれのインタフェースでも同じでなければならない。

5.1 アルゴリズム識別子

アルゴリズム識別子は、操作モードおよびリファレンスデータ長と併せて暗号アルゴリズムを示す 1 バイトの識別子でなければならない。表 7 は、PIV インタフェースで認識される可能性がある暗号アルゴリズムのアルゴリズム識別子を示したものである。その他のアルゴリズム識別子はすべて、将来の使用のために予約されている。

表 7. 暗号アルゴリズム識別子

アルゴリズム識別子	アルゴリズム – モード	リファレンスデータ長	必須(M)／オプション(O)
'01'	2-key トリプル DES– ECB	128 ビット	O
'02'	2-key トリプル DES– CBC	128 ビット	O
'03'	3-key トリプル DES– ECB	192 ビット（パリティビットを含む）	M
'04'	3-key トリプル DES– CBC	192 ビット（パリティビットを含む）	M
'05'	RSA	3072 ビット	O
'06'	RSA	1024 ビット	M
'07'	RSA	2048 ビット	O
'08'	AES-128 – ECB	24 バイト	O
'09'	AES-128 – CBC	24 バイト	O
'0A'	AES-192 – ECB	36 バイト	O
'0B'	AES-192 – CBC	36 バイト	O
'0C'	AES-256 – ECB	48 バイト	O
'0D'	AES-256 – CBC	48 バイト	O
'0E'	ECC:Curve P-224	224 ビット	O
'0F'	ECC:Curve K-233	233 ビット	O
'10'	ECC:Curve B-233	233 ビット	O
'11'	ECC:Curve P-256	256 ビット	O
'12'	ECC:Curve K-283	283 ビット	O
'13'	ECC:Curve B-283	283 ビット	O

アルゴリズム識別子が'00'である PIV カードアプリケーションでのデフォルトの暗号アルゴリズムは、3-key トリプル DES– ECB である。メッセージの埋め込みに関するテクニカルノートは、SP 800-73 と近く刊行される SP 800-78『Cryptographic Algorithms and Key Sizes for Personal Identity Verification』に同期して今後公開される予定である。

5.2 アプリケーション特性テンプレート

PIV カードアプリケーションは、選択された時に表 8 に記述するアプリケーション特性テンプレートを返さなければならない。

表 8. PIV カードアプリケーション特性テンプレート（タグ'61'）内のデータオブジェクト

記述	タグ	必須(M)／オプション(O)	コメント
アプリケーションのアプリケーション識別子	‘4F’	M	AID の PIX には、PIV カードアプリケーションのバージョンをコード化した情報が含まれる。
共存タグ割り当て局	‘79’	M	共存タグ割り当て権限テンプレート。表 9 を参照。
アプリケーションラベル	‘50’	O	アプリケーションを記述するテキスト（例: マンマシンインタフェース上での利用など）。
URL (Uniform resource locator)	‘5F50’	O	アプリケーションを記述した仕様への参照。

表 9. 共存タグ割り当て局テンプレート（タグ'79'）内のデータオブジェクト

記述	タグ	必須 (M)／オプション (O)	コメント
アプリケーション識別子	‘4F’	M	NIST は、この PIV RID を http:///csrc.nist.gov/piv-project に掲示し、テクニカルノートで公開する。

5.3 認証子

PIV クライアントアプリケーションプログラミングインタフェースで使用される認証子の BER-TLV は、表 10 に示す構造を持たなければならない。

表 10. 認証子テンプレート（タグ'67'）内のデータオブジェクト

記述	タグ	必須 (M)／オプション (O)	コメント
リファレンスデータ	‘81’	M	例: PIN 値や利用者確認のための応答など。
鍵参照	‘83’	M	表 12 を参照。

5.4 接続記述

PIV クライアントアプリケーションプログラミングインタフェースで使用される接続記述の BER-TLV は、表 11 に示す構造を持たなければならない。

表 11. 接続記述テンプレート（タグ'7F21'）内のデータオブジェクト

記述	タグ	必須 (M)／オプション (O)	コメント
インタフェースデバイス – PC/SC	‘81’	C	カードリーダの名前
インタフェースデバイス – SCP	‘82’	C	端末装置上のカードリーダ識別子
インタフェースデバイス – EMR	‘83’	C	無線送信を使用する非接触型接続
インタフェースデバイス – IR	‘84’	C	赤外線送信を使用する非接触型接続
インタフェースデバイス – PKCS#11	'85'	C	PKCS#11 インタフェース
インタフェースデバイス – CryptoAPI	'86'	C	CryptoAPI インタフェース
ネットワークノード – ローカル	‘90’	C	クライアントアプリケーションホストとカードリーダホストとの間にネットワークは存在しない
ネットワークノード – IP	‘91’	C	カードリーダホストの IP アドレス
ネットワークノード – DNS	‘92’	C	カードリーダホストのインターネットドメイン名
ネットワークノード – ISDN	‘93’	C	カードリーダがある端末装置の ISDN ダイヤル番号文字列

接続記述テンプレートには、'8x' 系列から選択した値と '9x' 系列から選択した値が最大で 1 つずつ現れなければならない。

例えば、'7F 21 0C 82 04 41 63 6D 65 91 04 81 06 0D 17' は、インターネットアドレス 129.6.13.23 にある総称的なカードリーダへの接続を表示している。また、例えば '7F 21 0B 82 01 00 93 06 16 17 12 34 56 7F' は、ダイヤル番号+1 617 123 4567 の携帯電話にある SIM (Subscriber Identity Module) への接続を示している。

第 5.1.1 節に記述した PIV クライアントアプリケーションプログラミングで pivConnect 入口点への引数として使用する場合、長さがゼロである '8x' 系列のデータオブジェクトとともに '9x' 系列のデータオブジェクトを指定すると、記述したノード上にある記述したタイプの使用可能なすべてのカードリーダを返す要求となる。したがって、'7F 21 04 81 00 90 00' は、クライアントアプリケーションを実行中のホスト上にあるすべての使用可能な PC/SC カードリーダのリストを要求することになる。

5.5 鍵参照

鍵参照は、暗号プロトコルで使用される PIV カードアプリケーション内の暗号対象物を示す 6 ビットの識別子である。1 バイトで表現する場合、鍵参照をビット 8 とビット 5～ビット 1 に設定し、ビット 7 とビット 6 は 0 に設定しなければならない。ビット 8 が 0 である場合、鍵参照はグローバルリファレンスデータを指定する。ビット 8 が 1 である場合、その鍵参照はアプリケーション固有のリファレンスデータを指定する。

表 12 は、PIV インタフェースで使用しなければならない鍵参照値を定義したものである。鍵参照値は、プライベートキーやシークレットキー(対称鍵)にのみ設定されている。その他のすべての PIV カードアプリケーション鍵参照値は、将来の使用のために予約されている。

表 12. PIV カードアプリケーション認証アルゴリズムおよび鍵参照

アルゴリズム識別子	鍵参照値	鍵参照名	認証可能エンティティ	セキュリティ条件の使用	リトライリセット値	非ブロック数
N/A	'00'	グローバル PIN	カード所有者	常に	プラットフォーム固有	プラットフォーム固有
N/A	'80'	アプリケーション PIN	カード所有者	常に	発行者固有	発行者固有
'06'	'9A'	PIV 認証鍵	PIV カードアプリケーション提供者	PIN	該当せず	該当せず
'00'	'9B'	PIV カードアプリケーション管理鍵	PIV カードアプリケーション管理者	常に	該当せず	該当せず
'06'	'9C'	PIV カードアプリケーションディジタル署名鍵	PIV カードアプリケーション管理者	PIN/常に	該当せず	該当せず
'06'	'9D'	PIV カードアプリケーション鍵管理鍵	PIV カードアプリケーション管理者	PIN	該当せず	該当せず

カード所有者のグローバル PIN は、PIV カードアプリケーションのアクセス制御規則によって参照可能であるが、PIV カードアプリケーションが現在選択されているアプリケーションである間は、現在のそのステータス、値は変更できず、リトライカウンタをリセットできない。

5.6 ステータスワード

ステータスワードは、クライアントアプリケーションプログラミングインタフェースの入口点、またはカードエッジのカードコマンドによって返される 2 バイト値でなければならない。ステータスワードの 1 バイト目を SW1 と呼び、2 バイト目を SW2 と呼ぶ。

表 13 は、クライアントアプリケーションプログラミングインタフェースとカードコマンドインタフェースのいずれにおいても、戻り値として使用されるすべての SW1 と SW2 のペアの認識される値とその解釈を示す。個々のクライアントアプリケーションプログラミングインタフェースの入口点またはカードコマンドの記述によって、返ってくるステータスワードの解釈に関する追加情報が提供される。

表 13. ステータスワード

SW1	SW2	意味
'61'	'xx'	正常実行。SW2 には、まだ利用可能な応答データのバイト数がコード化される。
'62'	'82'	データの終わりを検出した。
'63'	'xx'	警告。具体的な情報は入口点またはコマンドを参照。
'63'	'CX'	検証に失敗した。X は、今後許容されるリトライもしくはリセットの数を示す。

SW1	SW2	意味
‘68’	‘xx’	通信エラー。具体的な情報は入口点またはコマンドを参照。
‘69’	‘82’	セキュリティ条件を満たしていない。
‘69’	‘83’	認証処理がブロックされた。
‘69’	‘85’	使用条件を満たしていない。
‘6A’	‘80’	コマンドのデータフィールドに正しくないパラメタがある。
‘6A’	‘81’	機能がサポートされていない。
'6A'	'84'	メモリが不足している。
‘6A’	‘86’	P1 または P2 に正しくないパラメタがある。
‘6A’	‘88’	参照先のデータまたは参照元のデータが見つからない。
'90'	'00'	正常実行。

5.7 オブジェクト識別子

PIV カードアプリケーション内の各データオブジェクトには、NIST 個人検証アークからの ASN.1 OID および 3 バイトの BER-TLV タグが入る。このオブジェクト識別子の割り付けを表 6 に示す。

PIV クライアントアプリケーションプログラミングインタフェース上のデータオブジェクトは、その OID を使用して識別しなければならない。PIV クライアントアプリケーションプログラミングインタフェース上のオブジェクト識別子は、OID の整数部分をドットで区切った文字列でなければならない。例えば、PIV クライアントアプリケーションプログラミングインタフェース上での CHUID の OID 表現は '2.16.840.1.101.3.7.2.48.0' となる。

PIV カードアプリケーションのカードコマンドインタフェース上のデータオブジェクトは、その BER-TLV タグを使用してを識別しなければならない。例えば、PIV カードアプリケーションに対するカードコマンドインタフェースでは、CHUID は '5FC102' という 3 バイトの識別子によって識別される。

6. パート 3:最終インタフェースでのクライアントアプリケーションプログラミング

表 14 は、PIV クライアントアプリケーションプログラミングインタフェースの入口点をリストしたものである。

表 14. PIV クライアントアプリケーションプログラミングインタフェースの入口点

タイプ	名前
通信に関する入口点	pivConnect
	pivDisconnect
データアクセスに関する入口点	pivSelectCardApplication
	pivLogIntoCardApplication
	pivGetData
	pivLogoutOfCardApplication
暗号操作に関する入口点	pivCrypt
クレデンシャルの初期設定および管理に関する入口点	pivPutData
	pivGenerateKeyPair

6.1 通信に関する入口点

6.1.1 pivConnect

目的: クライアントアプリケーションプログラミングインタフェースを接続し、それによってクライアントアプリケーション自体を特定の ICC 上の PIV カードアプリケーションに接続する。

プロトタイプ:

status_word **pivConnect**(
IN Boolean **sharedConnection,**
INOUT sequence of bytes **connectionDescription,**
OUT handle **cardHandle**
);

パラメタ: **sharedConnection** TRUE の場合、他のクライアントアプリケーションが ICC に対して同時接続を確立できる。FALSE の場合、接続が確立されていれば、呼び出し側クライアントアプリケーションが ICC に対して排他的にアクセスする。

connectionDescription 接続記述データオブジェクト(タグ '7F21')。
表 11 を参照。

接続記述データオブジェクト内の '8x' データオブジェクトの値フィールドの長さがゼロの場合、'8x' 系列のデータオブジェクトのタグで指定されたタイプで '9x' のロケーションで利用可能なカードリーダのリストが connectionDescription に返さ

れる。

cardHandle 返された、特定の ICC、したがってカード自体への通信チャネルの秘密識別子。 cardHandle は、入口点の機能をどのカードに適用するかを識別するために、PIV クライアントアプリケーションプログラミングインタフェースの他のすべての入口点で使用される。

戻りコード: PIV_OK
PIV_CONNECTION_DESCRIPTION_MALFORMED
PIV_CONNECTION_FAILURE
PIV_CONNECTION_LOCKED

6.1.2 pivDisconnect

目的: PIV カードアプリケーションと PIV カードアプリケーションを含む ICC から、PIV アプリケーションプログラミングインタフェースの接続を切る。

プロトタイプ:
```
status_word pivDisconnect(
        IN handle cardHandle
);
```

パラメタ: **cardHandle** 操作対象カードの内部識別子(pivConnect が返したもの)。cardHandle の値は、pivDisconnect からの戻り時には未定義である。

戻りコード: PIV_OK
PIV_INVALID_CARD_HANDLE
PIV_CARD_READER_ERROR

6.2 データアクセスに関する入口点

6.2.1 pivSelectCardApplication

目的: 現在選択されているカードアプリケーションを設定する。

プロトタイプ:
```
status_word pivSelectCardApplication(
 IN handle            cardHandle,
 IN sequence of byte  applicationAID,
 OUT sequence of byte applicationProperties
);
```

パラメタ: **cardHandle** 操作対象カードの内部識別子(pivConnect が返したもの)。

applicationAID 現在選択されているカードアプリケーションとなるカードアプリケーションの AID。

applicationProperties 選択されているカードアプリケーション

のアプリケーション特性。表 8 を参照。

戻りコード: PIV_OK
PIV_INVALID_CARD_HANDLE
PIV_CARD_APPLICATION_NOT_FOUND
PIV_CARD_READER_ERROR

6.2.2 pivLogIntoCardApplication

目的: PIV カードアプリケーション内にアプリケーションセキュリティステータスを確立する。

プロトタイプ:
```
status_word pivLogIntoCardApplication(
        IN handle cardHandle,
        IN sequence of byte authenticators,
);
```

パラメタ: **cardHandle** 操作対象カードの内部識別子(pivConnect が返したもの)。

authenticators ゼロ個以上の、BER-TLV でコード化した認証子のシーケンス。カードアプリケーションに対してクライアントアプリケーションを認証することによって、カードアプリケーションで初期のセキュリティステータスを確立するために使用される。

戻りコード: PIV_OK
PIV_INVALID_CARD_HANDLE
PIV_AUTHENTICATOR_MALFORMED
PIV_AUTHENTICATION_FAILURE
PIV_CARD_READER_ERROR

6.2.3 pivGetData

目的: 指定されたデータオブジェクトのデータ内容全体を返す。

プロトタイプ:
```
status_word pivGetData(
 IN handle            cardHandle,
 IN string            OID,
 OUT sequence of byte data
);
```

パラメタ: **cardHandle** 操作対象カードの内部識別子(pivConnect が返したもの)。

OID データ内容を取得するオブジェクトのオブジェクト識別子は、文字列としてコード化する。例えば、以下のように記述する。
"2.16.840.1.101.3.7.1.1.2.2.1"

data 取得されたデータ内容。

戻りコード:
```
PIV_OK
PIV_INVALID_CARD_HANDLE
PIV_INVALID_OID
PIV_DATA_OBJECT_NOT_FOUND
PIV_SECURITY_CONDITIONS_NOT_SATISFIED
PIV_CARD_READER_ERROR
```

6.2.4 pivLogoutOfCardApplication

目的: PIV カードアプリケーションのアプリケーションセキュリティステータスをリセットする。正常にこの入口点から戻ったあとの、現在選択されているアプリケーションは、プラットフォームに依存する。

プロトタイプ:
```
status_word pivLogOutOfCardApplication(
 IN handle            cardHandle
);
```

パラメタ: **cardHandle** 操作対象カードの内部識別子(pivConnect が返したもの)。cardHandle は、この機能の実行後も引き続き有効である。

戻りコード:
```
PIV_OK
PIV_INVALID_CARD_HANDLE
PIV_CARD_READER_ERROR
```

6.3 暗号操作に関する入口点

6.3.1 pivCrypt

目的: バイトシーケンスの暗号化や署名などの暗号操作を実行する。

プロトタイプ:
```
status_word pivCrypt(
 IN handle            cardHandle,
 IN byte              algorithmIdentifier,
 IN byte              keyReference,
 IN sequence of byte  algorithmInput,
 OUT sequence of byte algorithmOutput
);
```

パラメタ: **cardHandle** 操作対象カードの内部識別子(pivConnect が返したもの)。

algorithmIdentifier 暗号操作に使用する暗号アルゴリズムの識別子。表 7 を参照。

keyReference 暗号操作に使用するカード上の鍵の識別子。表 12 を参照。

algorithmInput 暗号操作への入力として使用するバイトシーケンス。

algorithmOutput 暗号操作によって出力されるバイトシーケンス。

戻りコード: PIV_OK

PIV_INVALID_CARD_HANDLE
PIV_INVALID_KEYREF_OR ALGORITHM
PIV_SECURITY_CONDITIONS_NOT_SATISFIED
PIV_INPUT_BYTES_MALFORMED
PIV_CARD_READER_ERROR

エラー条件 PIV_INPUT_BYTES_MALFORMED は、要求された暗号アルゴリズムや鍵に対して、長さや埋め込みなど、処理すべきデータの特性に不適切なものがあったことを示す。

6.4 クレデンシャルの初期設定および管理に関する入口点

6.4.1 pivPutData

目的: 指定されたデータオブジェクトのデータ内容全体を、指定されたデータで置き換える。

プロトタイプ:

```
status_word pivPutData(
 IN handle            cardHandle,
 IN string            OID,
 IN sequence of byte  data
);
```

パラメタ: **cardHandle** 操作対象カードの内部識別子(pivConnect が返したもの)。

OID データ内容を置き換えるオブジェクトのオブジェクト識別子は、文字列としてコード化する。例えば、以下のように記述する。
"2. 16.840. 1. 101.3.7. 1.1.2.2. 1"

data 指定されたデータオブジェクトのデータ内容全体を置き換えるために使用されるデータ。

戻りコード:

PIV_OK
PIV_INVALID_CARD_HANDLE
PIV_INVALID_OID
PIV_DATA_OBJECT_NOT_FOUND
PIV_INSUFFICIENT_CARD_RESOURCE
PIV_CARD_READER_ERROR
PIV_SECURITY_CONDITIONS_NOT_SATISFIED

6.4.2 pivGenerateKeyPair

目的: 現在選択されているアプリケーションに、非対称鍵ペアを生成する。

指定された鍵参照が存在し、この鍵参照によって識別されるリファレンスデータに関連づけられた暗号メカニズムが、指定された暗号メカニズムと同一である場合、鍵参照に現在関連づけられている鍵ペア全体が、生成された鍵ペアによって置き換えられる。

プロトタイプ:

```
status_word pivGenerateKeyPair(
 IN handle            cardHandle,
 IN byte              keyReference,
 IN byte              cryptographicMechanism,
 OUT sequence of byte publicKey
);
```

パラメタ:

cardHandle 操作対象カードの内部識別子(pivConnect が返したもの)。

keyReference 生成された鍵ペアの鍵参照。

cryptographicMechanism 生成される鍵ペアのタイプ。表 20 を参照。

publicKey 生成された鍵ペアの公開鍵を定義する BER-TLV データオブジェクト。表 21 を参照。

戻りコード:

```
PIV_OK
PIV_INVALID_CARD_HANDLE
PIV_SECURITY_CONDITIONS_NOT_SATISFIED
PIV_INVALID_KEY_OR_KEYLAG_COMBINATION
PIV_UNSUPPORTED_CRYPTOGRAPHIC_MECHANISM
PIV_CARD_READER_ERROR
```

7. パート 3:最終インタフェースでの PIV カードアプリケーションカードコマンド

表 15 は、PIV カードアプリケーションを含む ICC のカードエッジで、PIV カードアプリケーションによって表されるカードコマンドの一覧である。PIV カードアプリケーションのカードコマンドはすべて、PIV カードアプリケーションによってサポートされなければならない。コマンド連鎖欄に「Yes」と示されているカードコマンドは、ISO/IEC 7816-4 [1] に定義された単一コマンドには長すぎるデータ文字列を送信するために、コマンド連鎖をサポートしなければならない。

表 15. PIV カードアプリケーションカードコマンド

タイプ	コマンド名	接触型インタフェース	非接触型インタフェース	使用時のセキュリティ条件	コマンド連鎖
データアクセスに関する PIV カードアプリケーションカードコマンド	SELECT	Yes	Yes	常に	No
	GET DATA	Yes	Yes	データに依存。表 1 を参照。	No
認証に関する PIV カードアプリケーションカードコマンド	VERIFY	Yes	No	常に	No
	CHANGE REFERENCE DATA	Yes	No	アプリケーション PIN	No
	RESET RETRY COUNTER	Yes	No	PIN ブロック解除キー	No
	GENERAL AUTHENTICATE	Yes	Yes(注を参照)	鍵に依存。	Yes
クレデンシャルの初期設定および管理に関する PIV カードアプリケーションカードコマンド	PUT DATA	Yes	No	PIV カードアプリケーション管理者	Yes
	GENERATE ASYMMETRIC KEY PAIR	Yes	No	PIV カードアプリケーション管理者	Yes

PIV カードアプリケーションは、表 15 の非接触型インタフェース欄に「No」と表示されているカードコマンドを非接触型インタフェースで受け取った場合、ステータスワード '6A 81'(機能がサポートされていない)を返さなければならない。

注:PIN を必要とする非対称鍵を使用する暗号プロトコルを、非接触型インタフェースで使用してはならない。

7.1 データアクセスに関する PIV カードアプリケーションのカードコマンド

7.1.1 SELECT カードコマンド

SELECT カードコマンドは、現在選択されているアプリケーションを設定する。PIV カードアプリケーションは、次のアプリケーション識別子

'A0 00 00 03 08 00 00 10 00 vv vv'

を SELECT コマンドのデータフィールドで指定して選択しなければならない。ここで 'vv vv' は、現在選択されているアプリケーションになる PIV カードアプリケーションのバージョンを示す。PIV カードアプリケーションの初期バージョンの AID は次のとおりである。

'A0 00 00 03 08 00 00 10 00 01 00'

どの ICC に存在する PIV カードアプリケーションも、最大 1 つでなければならない。右側を切り捨てたバージョン、つまり、2 バイトのバージョン番号'vv vv'のないバージョンを SELECT コマンドのデータフィールドに指定することによって、PIV カードアプリケーションを現在選択されているアプリケーションに設定することもできる。

'A0 00 00 03 08 00 00 10 00'

SELECT コマンドが正常に実行された時に現在選択されているアプリケーションとなる、PIV カードアプリケーションの完全な AID(2 バイトのバージョン番号を含む)は、アプリケーション特性テンプレートに返されなければならない。

現在選択されているアプリケーションが PIV カードアプリケーションである場合、データフィールドの AID が PIV カードアプリケーションの AID か、またはその右側を切り捨てたバージョンのいずれかであるような SELECT APPLICATION コマンドを発行すると、この PIV カードアプリケーションを引き続き現在選択されているアプリケーションとしなければならず、その PIV カードアプリケーションのどのセキュリティステータス標識の設定も変更してはならない。

現在選択されているアプリケーションが PIV カードアプリケーションである場合、データフィールドの AID が PIV カードアプリケーションの AID でも、その右側を切り捨てたバージョンのいずれでもない SELECT APPLICATION コマンドを発行すると、この PIV カードアプリケーションの選択が解除され、PIV カードアプリケーションのすべてのセキュリティステータス標識は FALSE に設定されなければならない。

コマンドシンタクス

CLA	'00'
INS	'A4'
P1	'04'
P2	'00'
Lc	アプリケーション識別子の長さ。
データフィールド	PIV カードアプリケーションのアプリケーション識別子。場合によっては、右側が切り捨てられる。
Le	アプリケーション特性テンプレートの長さ。

応答シンタクス

データフィールド	アプリケーション特性テンプレート
SW1-SW2	ステータスワード。

SW1	SW2	意味
'6A'	'82'	アプリケーションが見つからない。
'90'	'00'	正常実行。

7.1.2 GET DATA カードコマンド

GET DATA カードコマンドは、データフィールドでそのタグを指定した単一のデータオブジェクトのデータ内容を取得する。

コマンドシンタクス

CLA	'00'
INS	'CB'
P1	'3F'
P2	'FF'
Lc	'05'
データフィールド	表 16 を参照。
Le	取得するデータ内容のバイト数。

表 16. GET DATA カードコマンドのデータフィールド内データオブジェクト

名前	タグ	必須 (M)／オプション (O)	コメント
タグリスト	'5C'	M	取得するデータオブジェクトの BER-TLV タグ。表 6 を参照。

応答シンタクス

データフィールド	要求されたデータオブジェクトを値フィールドに含む、タグ'53'を持つ BER-TLV。
SW1-SW2	ステータスワード。

SW1	SW2	意味
'61'	'xx'	正常実行。SW2 には、まだ利用可能な応答データのバイト数がコード化される。
'69'	'82'	セキュリティステータスを満たしていない。
'6A'	'82'	データオブジェクトが見つからない。
'90'	'00'	正常実行。

7.2 認証に関する PIV カードアプリケーションのカードコマンド

7.2.1 VERIFY カードコマンド

VERIFY カードコマンドは、鍵参照によって示されるリファレンスデータと、当該コマンドのデータフィールドにある認証データとの比較をカード内で開始する。

PIV カードアプリケーションの VERIFY コマンドは、PIV カードアプリケーション固有の鍵参照、つまり、ローカルな鍵参照のみを検証しなければならない。

鍵参照に関連づけられているリトライカウンタの現在の値がゼロの場合、比較を実行してはならず、PIV カードアプリケーションはステータスワード '69 83' を返さなければならない。

コマンドデータフィールド内のリファレンスデータが第 3.5.3 節の基準を満たしていない場合、PIV カードアプリケーションはステータスワード '6A 80' を返さなければならない。

カードコマンドが正常に実行された場合、鍵参照のセキュリティステータスを TRUE に設定し、鍵参照に関連づけられているリトライカウンタを鍵参照に関連づけられているリセットリトライ値に設定しなければならない。

カードコマンドが失敗した場合、鍵参照のセキュリティステータスを FALSE に設定し、鍵参照に関連づけられているリトライカウンタを 1 つ減らさなければならない。

鍵参照に関連づけられているリトライカウンタとリセットリトライ値の初期値、つまり、鍵参照に関連づけられているリトライカウンタがゼロに達するまでの連続した失敗（リトライ）の回数は、発行者が決定する。

コマンドシンタクス

CLA	'00'
INS	'20'
P1	'00'
P2	鍵参照。表 12 を参照。
Lc	'08'
データフィールド	3.5.3 に記述した PIN リファレンスデータ。
Le	空。

応答シンタクス

SW1	SW2	意味
'63'	'CX'	検証に失敗した。X は、今後許容されるリトライの回数を示す。
'69'	'83'	認証方式がブロックされた。
'6A'	'80'	コマンドのデータフィールドに正しくないパラメタがある。
'6A'	'88'	鍵参照が見つからない。
'90'	'00'	正常実行。

7.2.2 CHANGE REFERENCE DATA カードコマンド

CHANGE REFERENCE DATA カードコマンドは、検証データとリファレンスデータの現在の値との比較を開始し、その比較に成功した場合は、リファレンスデータを新しいリファレンスデータで置き換える。この PIV カードアプリケーションコマンドで変更できるのは、PIV カードアプリケーション固有の鍵参照に関連づけられたリファレンスデータのみである。

PIV カードアプリケーションの CHANGE REFERENCE DATA コマンドは、PIV カードアプリケーション固有の鍵参照、つまり、ローカルな鍵参照に関連づけられているリファレンスデータのみを変更しなければならない。

鍵参照に関連づけられているリトライカウンタの現在の値がゼロの場合、この鍵参照に関連づけられているリファレンスデータを変更してはならず、PIV カードアプリケーションはステータスワード '69 83' を返さなければならない。

カードコマンドが正常に実行された場合、鍵参照のセキュリティステータスを TRUE に設定し、鍵参照に関連づけられているリトライカウンタを鍵参照に関連づけられているリセットリトライ値に設定しなければならない。

カードコマンドが失敗した場合、鍵参照のセキュリティステータスを FALSE に設定し、鍵参照に関連づけられているリトライカウンタを 1 つ減らさなければならない。

鍵参照に関連づけられているリトライカウンタとリセットリトライ値の初期値、つまり、鍵参照に関連づけられているリトライカウンタがゼロに達するまでの連続した失敗（リトライ）の回数は、発行者が決定する。

コマンドのコマンドフィールドにある現在のリファレンスデータか、新しいリファレンスデータのいずれかが第 3.5.3 節の基準を満たさない場合、PIV カードアプリケーションは、鍵参照に関連づけられているリファレンスデータを変更してはならず、ステータスワード '6A 80' を返さなければならない。

コマンドシンタクス

CLA	'00'
INS	'24'
P1	'00'
P2	鍵参照。表 12 を参照。
Lc	‘10’
データフィールド	現在の PIN リファレンスデータを、区切りなしで新しい PIN リファレンスデータと連結したもの。いずれの PIN も第 3.5.3 節の記述に従う。
Le	空。

応答シンタクス

SW1	SW2	意味
'63'	'CX'	検証に失敗した。X は、今後許容されるリトライの回数を示す。
‘69’	‘83’	認証方式がブロックされた。
‘6A’	‘80’	コマンドのデータフィールドに正しくないパラメタがある。
'6A'	'88'	鍵参照が見つからない。
'90'	'00'	正常実行。

7.2.3 RESET RETRY COUNTER カードコマンド

RESET RETRY COUNTER カードコマンドは、鍵参照のリトライカウンタを初期値にリセットし、鍵参照に関連づけられているリファレンスデータを変更する。このコマンドを使用すると、カード所有者が PIV カードアプリケーションの PIN を忘れた場合に PIN カードアプリケーションの復旧が可能になる。

PIV カードアプリケーションの RESET RETRY COUNTER コマンドは、PIV カードアプリケーション固有の鍵参照、つまり、ローカルな鍵参照に関連づけられているリトライカウンタのみをリセットしなければならない。

鍵参照に関連づけられているリセットカウンタの現在の値がゼロの場合、この鍵参照に関連づけられているリトライカウンタをリセットしてはならず、PIV カードアプリケーションはステータスワード '69 83' を返さなければならない。

カードコマンドが正常に実行された場合、鍵参照に関連づけられているリトライカウンタを、鍵参照に関連づけられているリセットリトライ値に設定しなければならない。鍵参照のセキュリティステータスとリセットカウンタは、いずれも変更してはならない。

カードコマンドが失敗した場合、鍵参照のセキュリティステータスを FALSE に設定し、鍵参照に関連づけられているリセットカウンタを 1 つ減らさなければならない。

鍵参照に関連づけられる初期のリセットカウンタ、つまり、鍵参照に関連づけられているリセットカウンタがゼロに達するまでの RESET RETRY COUNTER コマンドの失敗回数は、発行者が決定する。

コマンドのコマンドフィールドにあるリセットリトライカウンタのリファレンスデータ(PUK)か、新しいリファレンスデータ（PIN）のいずれかが第 3.5.3 節の基準を満たさない場合、PIV カードアプリケーションは、鍵参照に関連づけられているリトライカウンタをリセットしてはならず、ステータスワード '6A 80' を返さなければならない。

コマンドシンタクス

CLA	'00'
INS	'2C'
P1	'00'
P2	鍵参照。表 12 を参照。
Lc	‘10’
データフィールド	リセットリトライカウンタのリファレンスデータ(PUK)を区切りなしで新しいリファレンスデータ(PIN)と連結したもの。PUK と PIN はいずれも第 3.5.3 節の記述に従う。
Le	空。

応答シンタクス

SW1	SW2	意味
'63'	'CX'	検証に失敗した。X は、今後許容されるリトライの回数を示す。
‘69’	‘83’	認証方式がブロックされた。
‘6A’	‘80’	コマンドのデータフィールドに正しくないパラメタがある。
'6A'	'88'	鍵参照が見つからない。
'90'	'00'	正常実行。

7.2.4 GENERAL AUTHENTICATE カードコマンド

GENERAL AUTHENTICATE カードコマンドは、そのデータフィールドに指定されたデータを使用して認証プロトコルなどの暗号操作を実行し、その暗号操作の結果を応答データフィールドに返す。

GENERAL AUTHENTICATE コマンドは、クライアントアプリケーションに対してカードまたはカードアプリケーションを認証する場合（INTERNAL AUTHENTICATE）、カードに対してエンティティを認証する場合（EXTERNAL AUTHENTICATE）、およびカードとカード外部のエンティティとの間で相互認証を実行する場合（MUTUAL AUTHENTICATE）に使用しなければならない。

GENERAL AUTHENTICATE コマンドは、PIV クライアントアプリケーションプログラミングインタフェース上で署名機能を実現するために使用しなければならない。カードに送信されたデータは、カード外でハッシュ化される。

GENERAL AUTHENTICATE コマンドは、コマンドの長いデータフィールドを PIV カードアプリケーションに中断なく送信できるように、コマンド連鎖をサポートしている。GENERAL AUTHENTICATE コマンドの連鎖が終了する前に PIV カードアプリケーションが GENERAL AUTHENTICATE コマンド以外のカードコマンドを受け取った場合、PIV カードアプリケーションは、中断された連鎖内の最初のコマンドを受け取る直前の状態まで戻らなければならない。つまり、GENERAL AUTHENTICATE コマンドの連鎖が中断されても、PIV カードアプリケーションには影響を与えない。

コマンドシンタクス

CLA	'00'または '10' は、コマンドの連鎖を示す。
INS	'87'
P1	アルゴリズム参照
P2	鍵参照
Lc	データフィールドの長さ
データフィールド	表 17 を参照。
Le	無指定あるいは予想される応答の長さ

表 17. 動的認証テンプレート（タグ '7C'）内のデータオブジェクト

名前	タグ	必須 (M)／オプション (M)	記述
ウイットネス	'80'	C	事実を暴露することのない、事実に関する知識の実証。空のウイットネスは、ウイットネスの要求となる。
チャレンジ	'81'	C	認証プロトコルで使用される 1 つ以上の乱数またはバイトシーケンス。
レスポンス	'82'	C	認証プロトコルの応答ステップをコード化するバイトシーケンス。
コミットされたチャレンジ	'83'	C	1 つ以上のチャレンジを含む大きな乱数のハッシュコード。
認証コード	'84'	C	1 つ以上のデータフィールドとウィットネスデータオブジェクトのハッシュコード。

GENERAL AUTHENTICATE カードコマンドのデータフィールド内の動的認証テンプレート（タグ '7C'）に現れるデータオブジェクトは、実行される認証プロトコルに依存する。

応答シンタクス

データフィールド	無指定または認証関連データ
SW1-SW2	ステータスワード

SW1	SW2	意味
'61'	'xx'	正常実行。SW2 には、まだ利用可能な応答データのバイト数がコード化される。
‘69’	‘82’	セキュリティステータスを満たしていない。
‘6A’	‘80’	コマンドのデータフィールドに正しくないパラメタがある。
'6A'	'86'	P1 または P2 に正しくないパラメタがある。
'90'	'00'	正常実行。

7.3 クレデンシャルの初期設定および管理に関する PIV カードアプリケーションのカードコマンド

7.3.1 PUT DATA カードコマンド

PUT DATA カードコマンドは、PIV カードアプリケーション内の単一のデータオブジェクトのデータ内容を新しい内容で完全に置き換える。

コマンドシンタクス

CLA	‘00’または’10’は、コマンドの連鎖を示す。
INS	'DB'
P1	‘3F'
P2	‘FF’
Lc	データフィールドの長さ。
データフィールド	表 18 を参照。
Le	空。

表 18. PUT DATA カードコマンドのデータフィールド内のデータオブジェクト

名前	タグ	必須 (M)／オプション (O)	記述
タグリスト	'5C'	M	データ内容を置き換えるデータオブジェクトのタグ。表 6 を参照。
データ	‘53’	M	非構造化バイトシーケンスとしてタグ ‘53’ を持つデータ。

応答シンタクス

データフィールド	無指定または認証関連データ
SW1-SW2	ステータスワード

SW1	SW2	意味
'69'	'82'	セキュリティステータスを満たしていない。
'6A'	'84'	メモリが不足している。
'90'	'00'	正常実行。

7.3.2 GENERATE ASYMMETRIC KEY PAIR カードコマンド

GENERATE ASYMMETRIC KEY PAIR カードコマンドは、非対称鍵ペア（つまり、公開鍵とプライベート鍵）のリファレンスデータの生成とカード内での格納を開始する。生成された鍵ペアのうち公開鍵がコマンドへの応答として返される。鍵参照に現在関連づけられているリファレンスデータが存在する場合、このリファレンスデータ全体が生成されたデータによって置き換えられる。

コマンドシンタクス

CLA	'00'または '10' は、コマンドの連鎖を示す。
INS	'47'
P1	'00'
P2	生成された非対称鍵ペアに割り付けるゼロ以外の鍵参照。
Lc	データフィールドの長さ。
データフィールド	制御リファレンステンプレート。表 19 を参照。
Le	データオブジェクトテンプレートの公開鍵の長さ。

表 19. テンプレート（タグ 'AC'）内のデータオブジェクト

名前	タグ	必須 (M)／オプション (O)	記述
暗号メカニズム識別子	'80'	M	表 20 を参照。
パラメタ	'81'	C	暗号メカニズム固有

表 20. 暗号メカニズム識別子

暗号メカニズム識別子	記述	必須 (M)／オプション (O)	パラメタ
'00'-'04'	RFU		
'06'	RSA 1024	M	ビッグエンディアン形式でコード化されたオプションの公開鍵指数
'07'	RSA 2048	O	ビッグエンディアン形式でコード化されたオプションの公開鍵指数
'05'	RSA 3072	O	ビッグエンディアン形式でコード化されたオプションの公開鍵指数
'08'-'0D'	RFU		
'0E'	ECC:Curve P-224	O	なし
'0F'	ECC:Curve K-233	O	なし
'10'	ECC:Curve B-233	O	なし
'11'	ECC:Curve P-256	O	なし
'12'	ECC:Curve K-283	O	なし

'13'	ECC:Curve P-283	O	なし

その他の暗号メカニズム識別子値はすべて、将来の使用のために予約されている。

応答シンタクス

データフィールド	生成された鍵ペアの公開鍵のデータオブジェクト。表 21 を参照。
SW1-SW2	ステータスワード

表 21. テンプレート（タグ '7F49'）内のデータオブジェクト

名前	タグ
RSA の公開鍵データオブジェクト	
法	'81'
公開鍵指数	'82'
ECDSA の公開鍵データオブジェクト	
素数	'81'
第 1 係数	'82'
第 2 係数	'83'
ジェネレータ	'84'
順序	'85'
ポイント	'86'

SW1	SW2	意味
'61'	'xx'	正常実行。SW2 には、まだ利用可能な応答データのバイト数がコード化される。
'69'	'82'	セキュリティステータスを満たしていない。
'6A'	'80'	コマンドのデータフィールドに正しくないパラメタがある。例えば、認識されない暗号メカニズム。
'6A'	'86'	パラメタ P2 が正しくない。生成されるリファレンスデータの暗号メカニズムが指定された鍵参照のリファレンスデータの暗号メカニズムと異なる。
'90'	'00'	正常実行。

付録 A—PIV データモデル

PIV データモデル番号は 0x10 であり、データモデルバージョン番号は 0x01 である。

SP800-73 パート 3 仕様は、アプリケーションに PIV コンテナの内容の一部を読み取る機能を提供しない。コンテナ内の TLV 要素への個別アクセスはサポートしていない。パート 3 に適合したカードは、このデータモデルでのコンテナに対するリストの物理的な順番で、当該コンテナ内のすべての TLV 要素を返さなければならない。シングルチップ／デュアルインタフェースとデュアルチップのいずれの実装も実現可能でなければならない。シングルチップ／デュアルインタフェース構成では、どのインタフェースを使用しているかに関する情報を PIV カードアプリケーションに提供しなければならない。デュアルチップ構成では、各チップに個別の PIV カードアプリケーションをロードしなければならない。

バッファ記述	コンテナ ID	最大長（バイト数）	アクセス規則	接触型／非接触型	必須(M)／オプション(O)
カード機能コンテナ	0xDB00	266	常に読み込み	接触	M
カード所有者のユニークな識別子	0x3000	3377	常に読み込み	接触および非接触	M
PIV 認証に対する X.509 証明書	0x0101	1651	PIN	接触	M
カード所有者指紋	0x6010	7768	PIN	接触	M
印刷情報	0x3001	106	PIN	接触	O
カード所有者顔画像	0x6030	12704	PIN	接触	O
ディジタル署名に対する X.509 証明書	0x0100	1651	常に PIN	接触	O
鍵管理に対する X.509 証明書	0x0102	1651	PIN	接触	O
カード認証に対する X.509 証明書	0x0500	1651	常に	接触および非接触	O
セキュリティオブジェクト	0x9000	1000	常に読み込み	接触	M

次の表にあるデータ要素はすべて、オプションという指定がない限り必須であることに注意されたい。

カード機能コンテナ	0xDB00	常に読み込み	
データ要素(TLV)	タグ	タイプ	最大バイト数
カード識別子	0xF0	固定	21
機能コンテナバージョン番号	0xF1	固定	1
機能グラマーバージョン番号	0xF2	固定	1
アプリケーション CardURL	0xF3	可変	128
PKCS#15	0xF4	固定	1
登録済みデータモデル番号	0xF5	固定	1
アクセス制御規則テーブル	0xF6	固定	17
CARD APDU	0xF7	固定	0
リダイレクトタグ	0xFA	固定	0

機能タプル(CT)	0xFB	固定	0
ステータスタプル(ST)	0xFC	固定	0

カード機能コンテナ	0xDB00	常に読み込み	
データ要素 (TLV)	**タグ**	**タイプ**	**最大バイト数**
次の CCC	0xFD	固定	0
拡張アプリケーション CardURL（オプション）	0xE3	固定	48
セキュリティオブジェクトバッファ（オプション）	0xB4	固定	48
エラー検出コード	0xFE	LRC	0

カード所有者のユニークな識別子	0x3000	常に読み込み	
データ要素 (TLV)	**タグ**	**タイプ**	**最大バイト数**
FASC-N	0x30	固定テキスト	25
GUID	0x34	固定数値	16
有効期限	0x35	日付（YYYYMMDD）	8
認証鍵マップ（オプション）	0x3D	可変	512
発行者非対称署名	0x3E	可変	2816
エラー検出コード	0xFE	LRC	0

PIV 認証に対する X.509 証明書	0x0101	pkiCompute -PIN	
データ要素 (TLV)	**タグ**	**タイプ**	**最大バイト数**
証明書	0x70	可変	1856
認証情報	0x71	固定	1
MSCUID（オプション）	0x72	可変	38
エラー検出コード	0xFE	LRC	0

カード所有者指紋	0x6010	PIN	
データ要素 (TLV)	**タグ**	**タイプ**	**最大バイト数**
指紋 I	0xBC	可変	2000
指紋 II	0xBD	可変	2000
エラー検出コード	0xFE	LRC	0

印刷された情報	0x3001	PIN	
データ要素 (TLV)	タグ	タイプ	最大バイト数
名前	0x01	固定テキスト	32
従業員所属部署 1	0x02	固定テキスト	20
従業員所属部署 2	0x03	固定テキスト	20
有効期限	0x04	固定テキスト	9
政府機関カードシリアル番号	0x05	固定テキスト	10
発行者識別 I	0x06	固定テキスト	15
エラー検出コード	0xFE	LRC	0

カード所有者顔画像	0x6030	PIN	
データ要素 (TLV)	タグ	タイプ	最大バイト数
視覚検証用画像	0xBC	可変	12704
エラー検出コード	0xFE	LRC	0

ディジタル署名に対する X.509 証明書	0x0100	pkiCompute -PIN 常に	
データ要素 (TLV)	タグ	タイプ	最大バイト数
証明書	0x70	可変	1856
認証情報	0x71	固定	1
MSCUID（オプション）	0x72	可変	38
エラー検出コード	0xFE	LRC	0

鍵管理に対する X.509 証明書	0x0102	pkiCompute -PIN	
データ要素 (TLV)	タグ	タイプ	最大バイト数
証明書	0x70	可変	1856
認証情報	0x71	固定	1
MSCUID（オプション）	0x72	可変	38
エラー検出コード	0xFE	LRC	0

カード認証に対する X.509 証明書	0x0500	非対称 – pkiCompute – 常に 対称 – CCC / CHUID 参照	
データ要素 (TLV)	タグ	タイプ	最大バイト数
証明書	0x70	可変	1856
認証情報	0x71	固定	1
MSCUID（オプション）	0x72	可変	38
エラー検出コード	0xFE	LRC	0

セキュリティオブジェクト		0x9000 常に読み込み	
データ要素 (TLV)	タグ	タイプ	最大バイト数
コンテナ ID への DG のマッピング	0xBA	可変	100
セキュリティオブジェクト	0xBB	可変	900
エラー検出コード	0xFE	LRC	0

上で識別した証明書にある認証情報のバイトは、以下のようにコード化しなければならない。

```
CertInfo::= BIT STRING {
    CompressionTypeMsb(0),      // 0 =  圧縮なし、1 = gzip 圧縮
    CompressionTypeLsb(1),      // PIV アプリケーションの場合、'0'を設定しなければならない
    IsX509(2),                  // PIV アプリケーションの場合、'0'を設定しなければならない

    RFU3(3),
    RFU4(4),
    RFU5(5),
    RFU6(6),
    RFU7(7)
    }
```

付録 B—GENERAL AUTHENTICATE の使用例

B.1 PIV カードアプリケーション管理者の認証

PIV カードアプリケーション管理者は、チャレンジレスポンスプロトコルを使用して PIV カードアプリケーションから認証を受ける。PIV カードアプリケーションから取得したチャレンジは、クライアントアプリケーションによって暗号化され、PIV カードアプリケーション管理鍵への鍵参照である鍵参照'9B'に関連づけられている PIV カードアプリケーションに返される。PIV カードアプリケーションでは、このリファレンスデータと、鍵参照に関連づけられているアルゴリズム、つまり 3-key トリプル DES – ECB（アルゴリズム識別子 '00'）を使用してレスポンスを復号する。復号されたこの値が以前に取得したチャレンジと一致する場合は、PIV カードアプリケーション内で PIV カードアプリケーション管理者のセキュリティステータス標識が TRUE に設定される。

表 22 は、このチャレンジレスポンスプロトコルを実現するために、PIV カードアプリケーションに送られる GENERAL AUTHENTICATE カードコマンドを示す。

表 22. PIV カードアプリケーション管理者の認証

コマンド	応答	コメント
’00 87 00 00 04 7C 02 81 00’		クライアントアプリケーションが PIV カードアプリケーションからのチャレンジを要求する。
	‘7C 0A 81 08 01 02 03 04 05 06 07 08’	PIV カードアプリケーションからクライアントアプリケーションにチャレンジが返される。
’00 87 00 9B 0C 7C 0A 82 08 88 77 66 55 44 33 22 11’		クライアントアプリケーションはアルゴリズム ‘00’と鍵参照‘9B’ を参照して、チャレンジ（’88 77 66 55 44 33 22 11’）の暗号化を返す。表 7 および表 12 を参照。
	‘9000’	PIV カードアプリケーションは参照されているアルゴリズムと鍵を使用して ’88 77 66 55 44 33 22 11’ を復号し、’01 02 03 04 05 06 07 08’ を得た後、PIV カードアプリケーション管理者の認証に成功したことを示す。

B.2 PIV カードアプリケーションの認証

PIV カードアプリケーションは、まず PIV 認証鍵の X.509 証明書（OID 2.16.840.1.101.3.7.2.1.1）を取得し、この証明書の署名を検証することによって認証される。証明書が有効かつ最新であると見なすと、クライアントアプリケーションは、この証明書に関連づけられたプライベート鍵、つまり鍵参照 '9A'、アルゴリズム識別子 '06' を使用してチャレンジを暗号化することを PIV カードアプリケーションに要求する。レスポンスは、証明書の中にある公開鍵を使って復号される。復号されたレスポンスがチャレンジと一致すれば、PIV カードアプリケーションの正当性が確認される。

表 23 は、PIV カードアプリケーションの正当性確認を実現するために、PIV カードアプリケーションに送られる GENERAL AUTHENTICATE カードコマンドを示す。

表 23. GENERAL AUTHENTICATE を使用した、PIV カードアプリケーションの認証

コマンド	応答	コメント
’00 87 06 9A 0E 7C 0C 82 00 81 08 01 02 03 04 05 06 07 08’		クライアントアプリケーションは、鍵参照 ‘9A’ に関連づけられているリファレンスデータをアルゴリズム ‘06’ と一緒に使用するように指示して、PIV カードアプリケーションにチャレンジを送る。表 7 および表 12 参照。
	’7C 0A 82 08 88 77 66 55 44 33 22 11’	PIV カードアプリケーションは、指示された鍵参照データとアルゴリズムを使用して暗号化したチャレンジ（’88 77 66 55 44 33 22 11’）を返す。

同じように GENERAL AUTHENTICATE を使用して、PIV カードアプリケーションがハッシュなどのバイトシーケンスの署名を行うことも可能である。必要な作業は、使用するアルゴリズムと鍵をそれぞれ P1 パラメタと P2 パラメタに設定することによって、指示することだけである。

この例では、説明のために 8 バイトのチャレンジとレスポンスのみを 1024 ビットの RSA 鍵で使用していることに注意されたい。実際には、この暗号アルゴリズムにさらに適合した質問と応答が使用されるであろう。

付録 C—PIV 認証のユースケース

本節では、PIV カードがサポートする使用法やふるまいについてのガイダンスを提供するために、PIV 認証のユースケースとアプリケーションシナリオを記述する。FIPS 201 は、PIV 認証を「PIV カードを提示するカード所有者の身元について信頼を確立するプロセス」であると記述している。PIV カードを使用する基本的な目的は、保護された資源やファシリティへのアクセスを管理しているシステムや担当者に対して、カード所有者の身元を認証することである。この最終目標は、以下に記述する正当性確認ステップの 1 つ以上をさまざまな形で組み合わせることによって達成可能である。

+ カードの正当性確認（CardV）— これは、PIV カードが真正であり（つまり、偽造カードでなく）、タンパーや改変が行われていないことを検証するプロセスである。カードの正当性確認メカニズムには次のものなどがある。

  - FIPS 201 第 4.1.2 節に従った、PIV カードのタンパープルーフおよびタンパーレジスタントの目視検査。
  - 対称鍵による、チャレンジ・レスポンス暗号化スキームの使用。
  - PIV カード内部に組み込まれたプライベート鍵の正当性を確認するための、非対称認証スキームの使用。

+ クレデンシャルの正当性確認（CredV）— これは、PIV カードに保持されているさまざまなタイプのクレデンシャル（視覚的なクレデンシャル、CHUID、バイオメトリック、PIV 鍵、証明書など）を検証するプロセスである。信用情報の正当性確認メカニズムには次のものなどがある。

  - PIV カードの視覚的要素（存在する場合は、写真、印刷されている氏名、地位など）の目視検査。
  - PIV カード上の証明書の検証。
  - PIV バイオメトリックおよび CHUID 上の署名の検証。
  - 有効期限のチェック。
  - PIV カード上の証明書の取り消しステータスのチェック。

+ カード所有者の正当性確認（HolderV）— これは、PIV カードがその正当な所有者に所持されていることを明確にするためのプロセスである。これまで、次の要素の 1 つ以上を使用して身元認証が行われてきた。a) 本人の持っているもの、b) 本人の知っている情報、c) 本人の個人的特徴。認証プロセスの保証は、使用する要素の数とともに高まる。PIV カードの場合、これらの 3 つの要素は次のように解釈される。a) 本人の持っているもの – PIV カードの所持、b) 本人の知っている情報 – PIN を知っていること、c) 本人の個人的特徴 – カード所有者の外見的特徴、カード所有者がその場で提供した指紋サンプル。したがって、PIV カード所有者の正当性確認メカニズムには次のものなどがある。

  - カード所有者による PIV カードの提示。
  - カード所有者の外見的特徴と PIV カード上の写真との照合。

- 提供された PIN と PIV カード上の PIN との照合。
- カード所有者がその場で提供した指紋サンプルと PIV カードに埋め込まれているバイオメトリック情報との照合。

C.1 ユースケース図

本節では、PIV カードの相互運用および認証に伴うアクティビティや相互作用について述べる。ユースケースは、認証側がそのシステムやファシリティへのアクセスを提供するために、カード所有者をどのように認証するか（どの政府機関がカードを発行したかにかかわらず）を表現している。このアクティビティや相互作用は、機能ユースケース図で表現されている。これらのユースケース図は、シンタクス上のコマンドや API 関数名を示すためのものではない。

本節で記述する PIV 認証メカニズムはそれぞれ、カード、クレデンシャル、およびカード所有者の正当性確認を実行する、1 つ以上の正当性確認ステップのシーケンスに分割することが可能である。ユースケース図の中では、カード、クレデンシャル、およびカード所有者の正当性確認であることを表すために、正当性確認ステップにそれぞれ「CardV」、「CredV」、「HolderV」とマークする。

信頼側当事者は、所定の PIV 認証メカニズムでの正当性確認ステップの実際のシーケンスによって実現される保証に応じて、保護された資源へのアクセスの許可についてリスク分析に基づいて適切な判断を下すことが可能である。

C.1.1 PIV の視覚的クレデンシャルを使用した認証

これは、人間の警備員が PIV カードに保持されている視覚的なクレデンシャルを使用してカード所有者を認証するユースケースである。これを図 C-1 に示す。

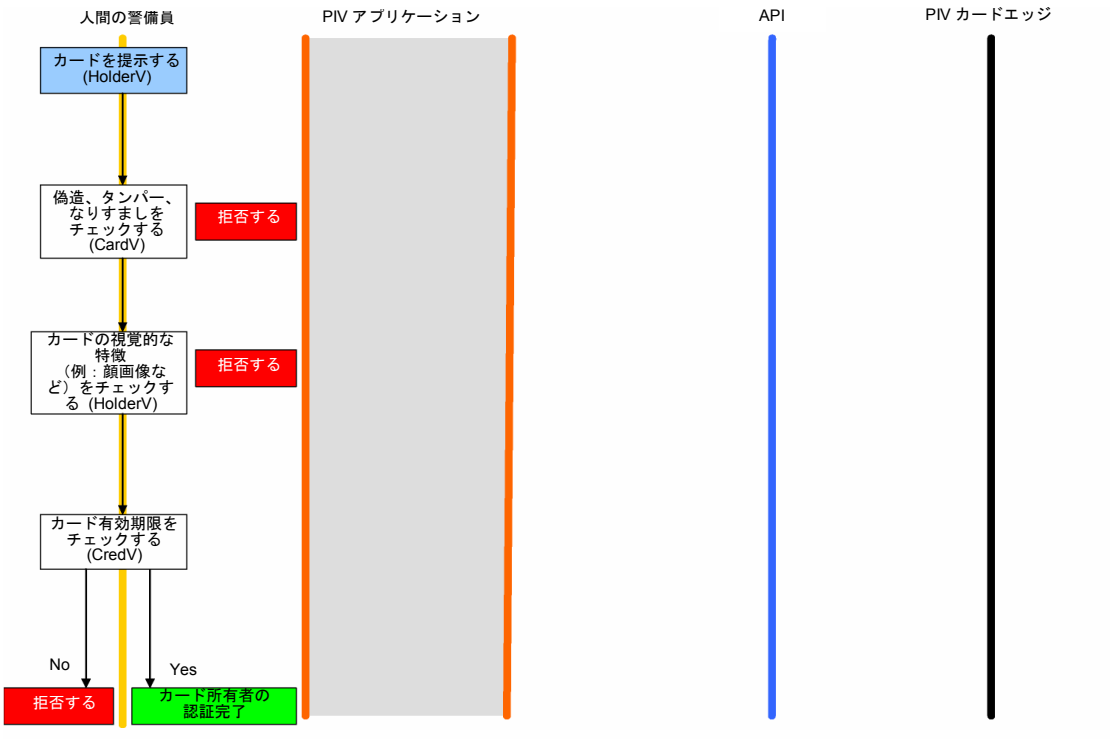

図 C-1：PIV の視覚的クレデンシャルを使用した認証

C.1.2 PIV CHUID を使用した認証

PIV CHUID を使用した認証には、いくつかのバリエーションがある。PIV カードを使用して PACS の Low 保証プロファイルを実装する方法を図 C-2 に示す。PIV アプリケーションからローカルシステムに送信されなくてはならない最低限の認証データは、アプリケーションに依存しているため、この仕様では定義されない。

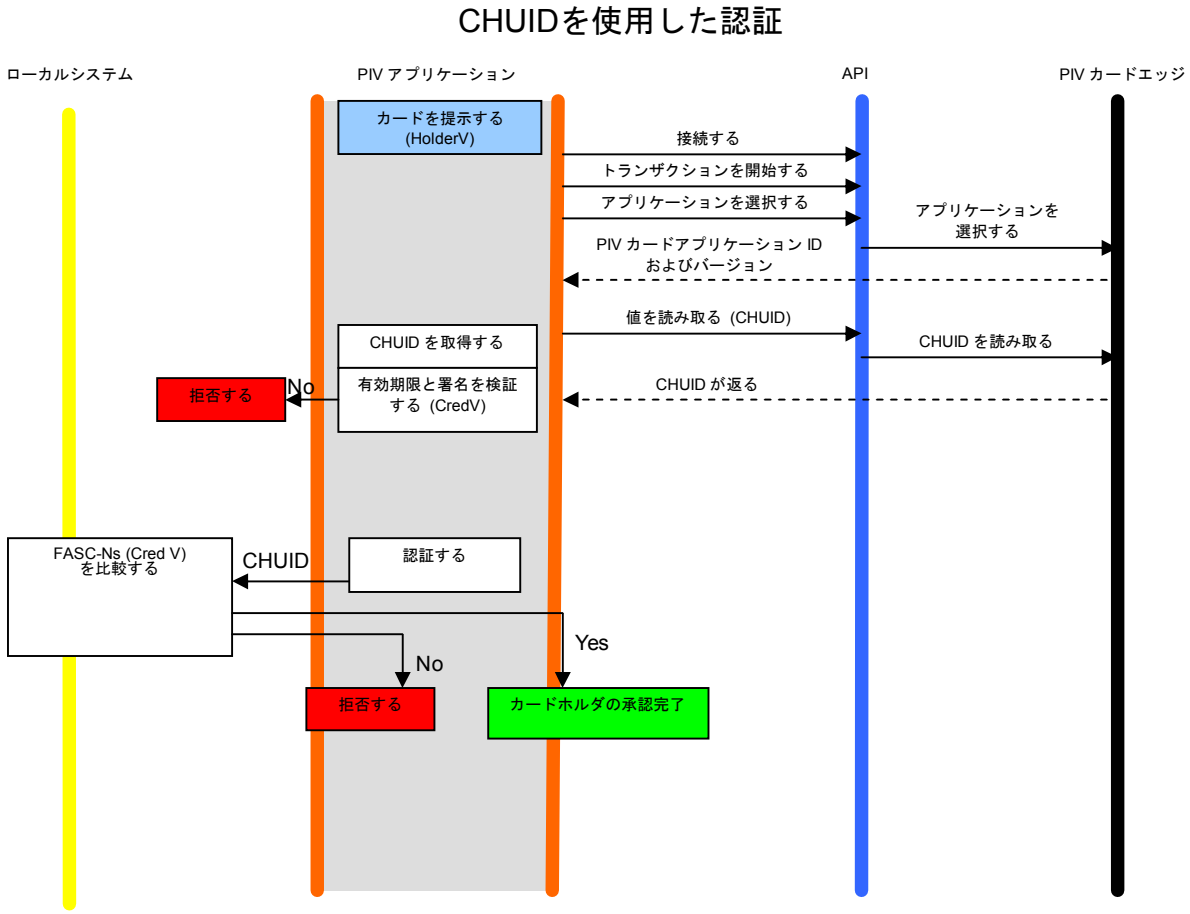

図 C-2：PIV CHUID を使用した認証

C.1.3 PIV バイトオメトリクスを使用した認証

PIV バイオメトリックを使用した認証の一般的なユースケースを図 C-3 に示す。

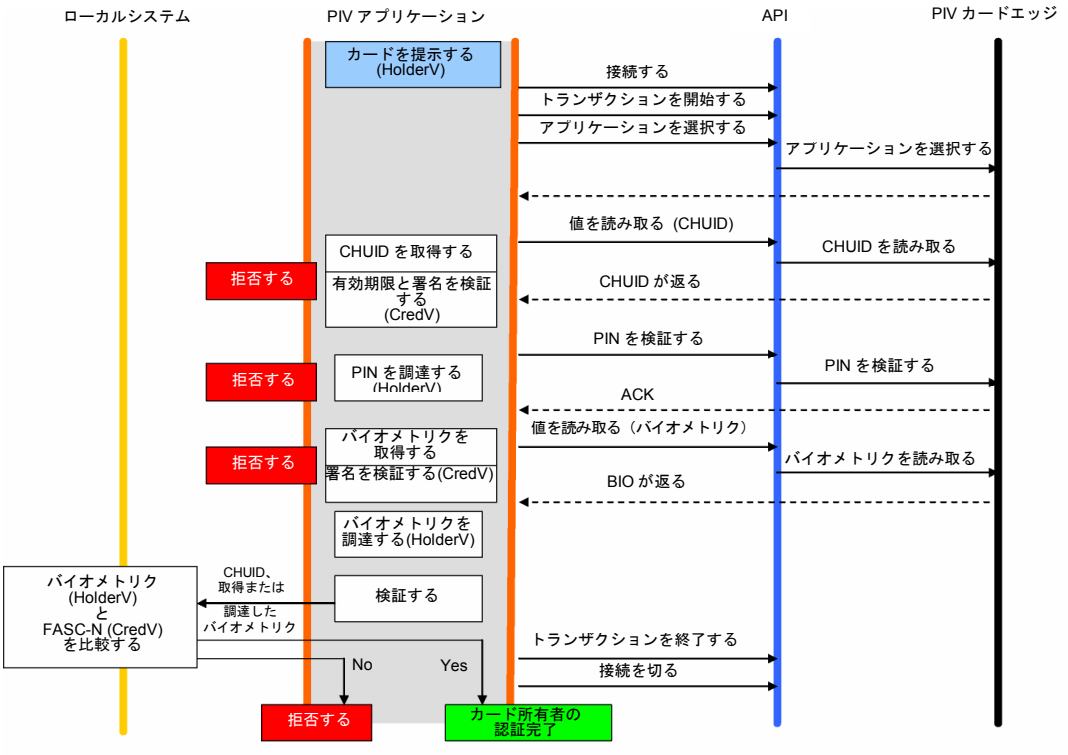

図 C-3：PIV バイトオメトリクスを使用した認証

係員が立ち会う環境で、人間がプロセスを監督しながらその場でバイオメトリックサンプルを収集する場合、PIV バイオメトリックを使用した認証の保証がさらに高まる可能性がある。このユースケースを図 C-4 に示す。

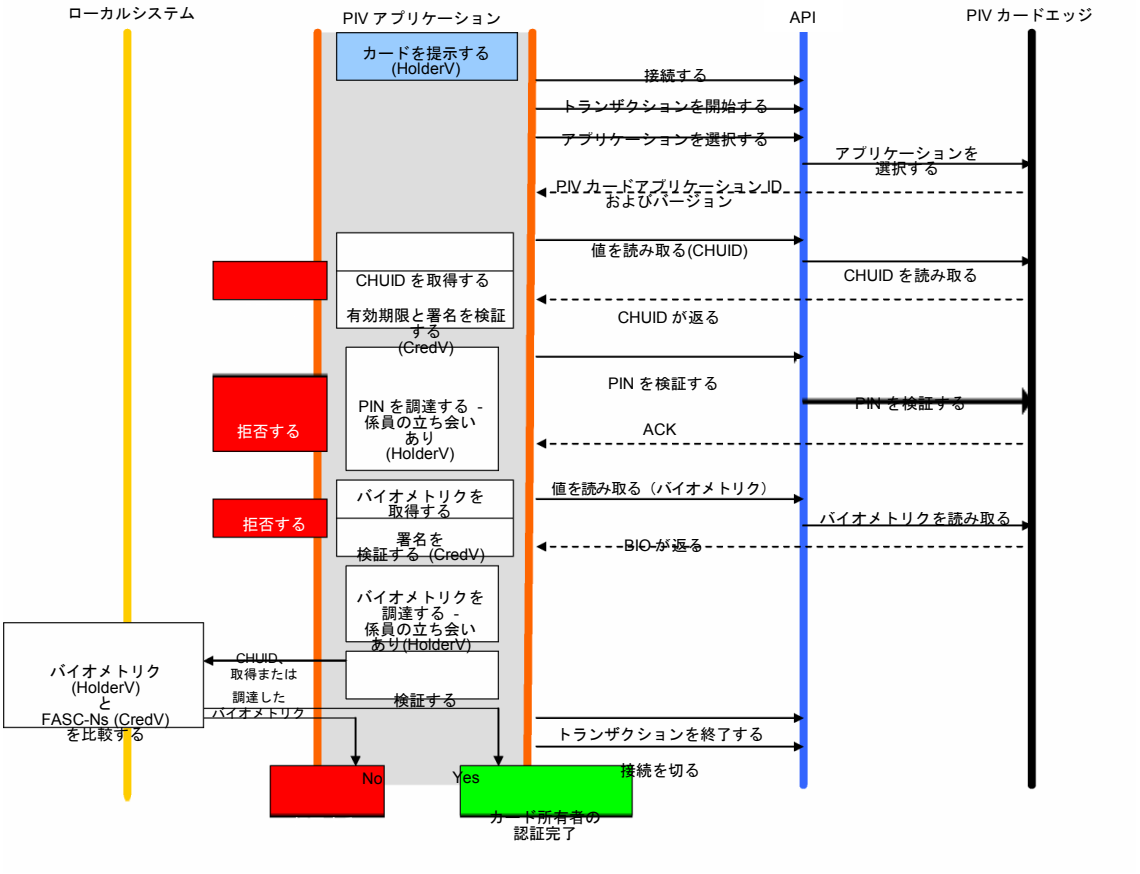

図 C-4：PIV バイトオメトリクスを使用した認証（係員が立ち会う場合）

C.1.4 PIV 認証鍵を使用した認証

PIV 認証鍵を使用した認証のユースケースを図 C-5 に示す。

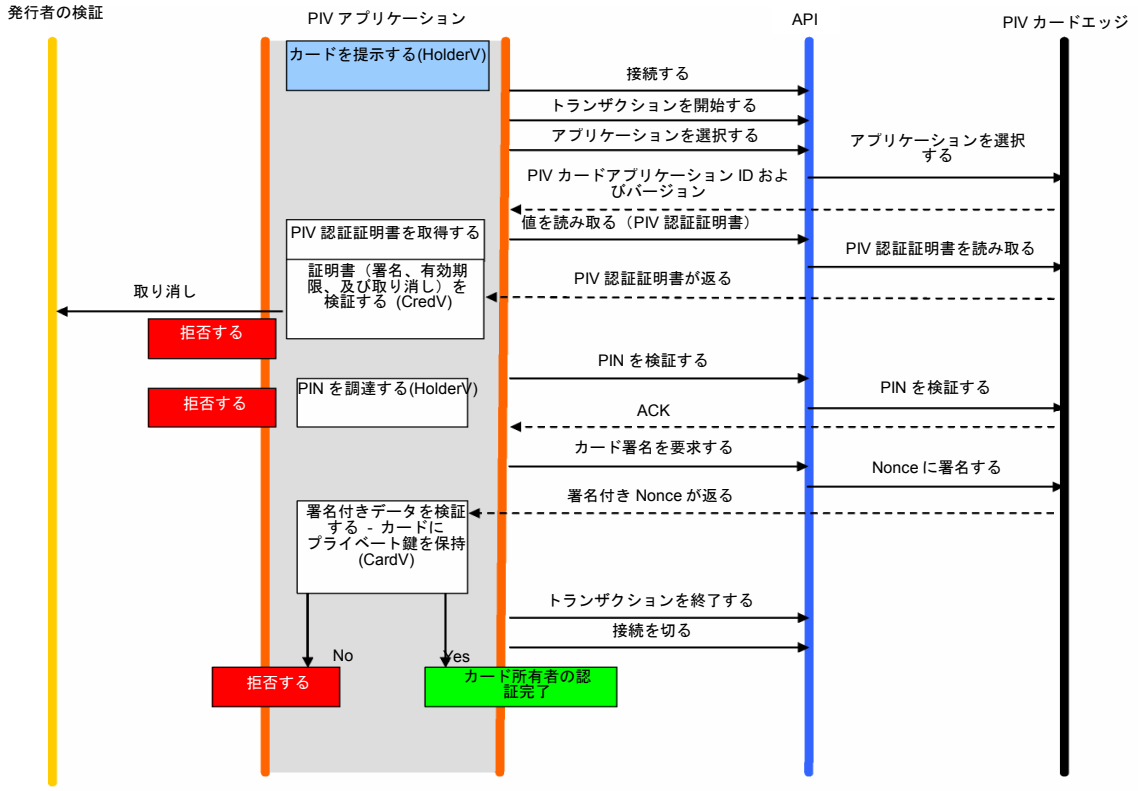

図 C-5：PIV 認証鍵を使用した認証

C.2 要約表

次の表は、本節で既に述べたそれぞれの PIV 認証メカニズムに含まれる正当性確認アクティビティのタイプを要約したものである。

PIV 認証メカニズム	カード正当性確認ステップ(CardV)	クレデンシャル正当性確認ステップ(CredV)	カード所有者正当性確認ステップ(HolderV)
PIV 視覚認証	1. 偽造、改ざん、およびねつ造のチェック	1. 有効期限のチェック	カードの所持 カード上の視覚的特徴とカード所有者との照合
PIV CHUID		有効期限のチェック CHUID 署名のチェック（オプション）	カードの所持
PIV バイオメトリック（係員不在）		有効期限のチェック CHUID 署名のチェック（オプション） PIV バイオメトリック署名のチェック（オプション）	カードの所持 PIN の照合 カード所有者のバイオメトリックと PIV バイオメトリックの照合
PIV バイオメトリック（係員立会い）		有効期限のチェック CHUID 署名のチェック（オプション） PIV バイオメトリック署名のチェック（オプション）	カードの所持 PIN の照合 カード所有者のバイオメトリックと PIV バイオメトリックの照合 *（係員立会いのもとで）*

PIV 認証メカニズム	カード正当性確認ステップ(CardV)	クレデンシャル正当性確認ステップ(CredV)	カード所有者正当性確認ステップ(HolderV)
PIV 認証鍵	1. PIV 非対称鍵でのチャレンジレスポンスを実行し、応答があり次第署名の正当性を確認する	カード有効期限のチェック PIV 認証証明書の認証	カードの所持 所有者が提供した PIN と PIV PIN との照合

付録 D—用語、頭字語、および表記法

D.1 用語

アプリケーション識別子 (Application Identifier)	ISO/IEC 7816-4 で定義された、カードアプリケーションのグローバルにユニークな識別子。
アプリケーションセッション (Application Session)	カードセッションの中で、あるカードアプリケーションが選択されてから、別のカードアプリケーションが選択されるまで、またはカードセッションが終了するまでの期間。
認証可能エンティティ (Authenticatable Entity)	カードアプリケーションの認証プロトコルに正常に関与できるエンティティ。
BER-TLV データオブジェクト (BER-TLV Data Object)	ISO/IEC 8825-2 に従ってコード化されたデータオブジェクト。
カード (Card)	IC（集積回路）カード。
カードアプリケーション (Card Application)	アプリケーション識別子を使用して選択できる、一連のデータオブジェクトとカードコマンド。
カードインタフェースデバイス (Card Interface Device)	IC カードおよびその中のカードアプリケーションをクライアントアプリケーションに接続する電子デバイス。
カードリーダ (Card Reader)	「カードインタフェースデバイス」と同義。
クライアントアプリケーション (Client Application)	コンピュータ上で、カードインタフェースデバイスと通信しながら稼働するコンピュータプログラム。
データオブジェクト (Data Object)	カードコマンドインタフェースで見られる情報項目であり、名前、論理的な内容の記述、書式、およびコーディングが規定されているもの。
インタフェースデバイス (Interface Device)	「カードインタフェースデバイス」と同義。
鍵参照 (Key Reference)	認証プロトコルや署名プロトコルなどの暗号プロトコルで使用される暗号鍵情報の 6 ビットの識別子。
MSCUID	Common Access Card and Government Smart Card Interoperability Specification と互換性のある任意のレガシーの識別子。
オブジェクト識別子 (Object Identifier)	ISO/IEC 8824-2 で定義された、データオブジェクトのグローバルにユニークな識別子。

参照データ (Reference Data)	認証プロトコルや署名プロトコルなどの暗号プロトコルを実行するのに使用される暗号情報。
ステータスワード (Status Word)	任意のコマンドを処理したあとに IC カードが返す 2 バイトで、処理の正常終了またはこの処理中に検出された誤りを通知する。
テンプレート (Template)	値フィールドに特定の BER-TLV データオブジェクトが格納される、(構成された)BER-TLV データオブジェクト。

D.2 略語

AES	Advanced Encryption Standard
AID	Application Identifier（アプリケーション識別子）
APDU	Application Protocol Data Unit（アプリケーションプロトコルデータ単位）
API	Application Programming Interface（アプリケーションプログラミングインタフェース）
ASN.1	Abstract Syntax Notation
BER	Basic Encoding Rules（基本コード化規則）
BSI	Basic Services Interface（基本サービスインタフェース）
CBC	Cipher Block Chaining mode
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）
CCC	Card Capability Container（カード機能コンテナ）
CLA	Class (first) byte of a card command（カードコマンドのクラス（先頭）バイト）
CHUID	Card Holder Unique IDentifier（カード所有者のユニークな識別子）
DES	Data Encryption Standard
DNS	Domain Name Server（ドメインネームサーバー）
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography（楕円曲線暗号技術）
ECDSA	Elliptic Curve Digital Signature Algorithm
EMR	Electro Magnetic Radiation（電磁放射）
FASC-N	Federal Agency Smart Credential Number（連邦機関スマートクレデンシャル番号）
FIPS	Federal Information Processing Standards（連邦情報処理規格）
FISMA	Federal Information Security Management Act（連邦情報セキュリティマネジメント法）
GSC-IAB	Government Smart Card Interagency Advisory Board（政府スマートカード省庁間諮問委員会）
GSC-IS	Government Smart Card Interoperability Specification（政府スマートカード相互運用性仕様）

GUID	Global Unique Identification Number
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
INS	Instruction (second) byte of a card command（カードコマンドの命令（第 2）バイト）
IP	Internet Protocol
IR	Infra Red（赤外線）
ISDN	Integrated Services Digital Network（ISDN ネットワーク）
ISO	International Standards Organization（国際標準化機構）
LSB	Least Significant Bit（最下位ビット）
MRTD	Machine Readable Travel Document（機械可読式渡航文書）
MSB	Most Significant Bit（最上位ビット）
OID	Object Identifier（オブジェクト識別子）
OMB	Office of Management and Budget（行政管理予算局）
P1	First parameter of a card command（カードコマンドの第１パラメタ）
P2	Second parameter of a card command（カードコマンドの第 2 パラメタ）
PACS	Physical Access Control System（物理的アクセス制御システム）
PC/SC	Personal Computer/Smart Card（パーソナルコンピュータ／スマートカード）
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIX	Proprietary Identifier eXtension（拡張専有識別子）
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure（公開鍵基盤）
PUK	PIN Unblocking Key（PIN ブロック解除鍵）
RFU	Reserved for Future Use
RID	Registered application provider Identifier（登録済みアプリケーション提供者識別子）
RSA	Rivest, Shamir, Aldeman

SCEPACS	Smart Card Enabled Physical Access Control System
SCP	ETSI Smart Card Project（ETSI スマートカードプロジェクト）
SP	Special Publication
SW 1	First byte of a two-byte status word（2 バイトステータスワードの第 1 バイト）
SW2	Second byte of a two-byte status word（2 バイトステータスワードの第 2 バイト）
TIG	Technical Implementation Guidance（技術実装ガイダンス）
TLV	Tag-Length-Value（タグ－長さ－値）
URL	Uniform Resource Locator
VM	Virtual Machine（仮想マシン）

D.3 表記法

16 個の 16 進数は、英数字（0、1、2…、A、B、C、D、E、および F）を使用して表記しなければならない。1 バイトは、2 桁の 16 進数で構成される（例えば、‘2D’）。バイトシーケンスは一重引用符で囲む場合があり、例えば、'A0’ ‘00’ ‘00’ ‘01’ ‘16' という個別のバイトシーケンスではなく、'A0 00 00 01 16'と表記する。

バイトは、ビット 8 からビット 1 までで表現することもできる。この場合、バイトのビット 8 が最上位ビット（MSB）、ビット 1 が最下位ビット（LSB）である。テキストや図の表現では、左端のビットが MSB となる。したがって、例えば ‘80’ の最上位ビット（ビット 8）は 1、最下位ビット（ビット 1）は 0 である。

将来の使用のために予約済み（RFU）として規定されているバイトにはすべて '00' を設定し、RFU として規定されているビットにはすべて 0 を設定しなければならない。

特に断りがない限り、長さはすべてバイト数で表すものとする。

テンプレート内のデータオブジェクトは、必須（M）、オプション（O）、または条件付き（C）として記述される。「必須」は、そのデータオブジェクトがテンプレート内に現れなければならないことを意味する。「オプション」は、そのデータオブジェクトがテンプレート内に現れてもよいことを意味する。条件付きデータオブジェクトの場合は、そのデータオブジェクトが必要となる条件を表の脚注で規定する。

その他の表では、「必須（M）／オプション（O）」欄によって、存在しなければならない（M）、または存在してもよい（O）PIV カードアプリケーションの特性を識別する。

BER-TLV データオブジェクトのタグは、前述したようなバイトシーケンスで表現される。したがって、例えば‘4F’はアプリケーション識別子の産業間データオブジェクトタグであり、‘7F 60’ はバイオメトリック情報テンプレートの産業間データオブジェクトタグである。

本標準における「しなければならない（MUST）」、「してはならない（MUST NOT）」、「必要がある（REQUIRED）」、「しなければならない（SHALL）」、「してはならない（SHALL NOT）」、「するべき

（SHOULD）」、「するべきでない（SHOULD NOT）」、「推奨される（RECOMMENDED）」、「してもよい（MAY）」、および「オプションである（OPTIONAL）」という各キーワードは、IETF RFC 2119、Key Words for Use in RFCs to Indicate Requirement Levels [6] の記述に従って解釈される。

付録 E—リファレンス

[1] ISO/IEC 7816 (Parts 4, 5, 6, 8, and 9), Information technology — Identification cards — Integrated circuit(s) cards with contacts.

[2] ISO/IEC 8824-2:2002, Information technology -- Abstract Syntax Notation One (ASN.1):Information object specification.

[3] ISO/IEC 8825-1:2002, Information technology — ASN.1 encoding rules:Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

[4] NIST Federal Information Processing Standards Publication 201, *Personal Identity Verification for Federal Employees and Contractors,* February, 2005.

[5] PACS v2.2, *Technical Implementation Guidance:Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 27, 2004.

[6] IETF RFC 2119, "Key Words for Use in RFCs to Indicate Requirement Levels," March, 1997.

[7] Government Smart Card Interoperability Specification, Version 2.1, NIST Interagency Report 6887 – 2003 Edition, July 16, 2003.

[8] PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version - 1.1 Date - October 01, 2004. Published by authority of the Secretary General, International Civil Aviation Organization.