FIPS PUB 201-1

Change Notice 1

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
（連邦情報処理規格）

連邦職員および委託業者の
アイデンティティの検証

米国国立標準技術研究所
情報技術ラボラトリ
コンピュータセキュリティ部門
Gaithersburg, MD 20899-8900

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 A. Jeffrey

謝辞

NIST は、連邦個人認証委員会（Federal Identity Credentialing Committee、以下、FICC と称す）およびスマートカードに関する省庁間諮問委員会（Smart Card Interagency Advisory Board、以下、IAB と称す）に対し、本規格の基盤となった技術フレームワークの開発に関する多大な貢献に感謝する。

本規格の策定過程においてワークショップに参加され、貴重な技術的提案をくださった諸氏に心より感謝する。また、準備草案レビュー期間に政府機関および業界団体から寄せられたコメントに対しても謝意を表すものである。

まえがき

米国国立標準技術研究所（National Institute of Standards and Technology、以下、NISTと称す）の連邦情報処理規格（Federal Information Processing Standards Publication、以下、FIPS PUBと称す）シリーズは、2002年施行の連邦情報セキュリティマネジメント法（Federal Information Security Management Act of 2002、以下、FISMAと称す）の規定に基づいて採択および公布される規格およびガイドラインに関する公式刊行物のシリーズである。

FIPSの刊行物に対するコメントを歓迎する。コメントは、「Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900」宛に送付されたい。

Dr. Shashi Phoha, Director
情報技術ラボラトリ

概要

本規格は、連邦職員および委託業者が共通的に使用する身元証明手段の標準について、アーキテクチャおよび技術的要件を定めるものである。総体的な目標は、連邦政府の管理下にある公的施設への物理的アクセスおよび政府情報システムへの電子的アクセスを求める個人について、当該個人が主張するアイデンティティを効率的に検証することにより、複数のアプリケーションにおいて適切なセキュリティ保証を実現することにある。

本規格は大きく2つのセクションより構成される。第1部では、国土安全保障に関する大統領令12（HSPD 12：Homeland Security Presidential Directive 12）の管理目標およびセキュリティ目標に適合する連邦政府機関のアイデンティティティティティ検証システムに対する最低限の要件を説明する。これにはアイデンティティの立証、登録、および発行に関する要件を含む。第2部では、連邦政府省庁および政府機関における個人アイデンティティの検証（PIV：Personal Identity Verification）システム間での技術的な相互運用性をサポートする詳細仕様を示す。これには、カードへのアイデンティティクレデンシャルの格納、そこでの処理、およびそこからの取得を安全に実行するために必要な（REQUIRED）カード要素、システムインタフェース、およびセキュリティ管理策に関する説明を含む。カードの物理的特性、格納媒体、およびアイデンティティクレデンシャルを構成するデータ要素は、本規格において指定する。スマートカードへのアイデンティティクレデンシャルを格納およびそこからの抽出のためのインタフェースおよびカードアーキテクチャは、SP 800-73『個人アイデンティティ検証インタフェース（Interfaces for Personal Identity Verification）』において指定される。同様に、バイオメトリクス情報のインタフェースおよびデータ形式は、SP 800-76『アイデンティティの検証における生体認証データ仕様（Biometric Data Specification for Personal Identity Verification）』において指定される。

本規格では、連邦政府省庁および政府機関におけるアクセス制御のポリシーまたは要件については指定しない。

*キーワード:*アーキテクチャ、認証、承認、バイオメトリクス、クレデンシャル、暗号技術、連邦情報処理規格（FIPS：Federal Information Processing Standards）、HSPD 12、識別、アイデンティティ、インフラストラクチャ、モデル、個人のアイデンティティの検証（PIV：Personal Identity Verification）、有効性確認、検証。

FIPS PUB 201
2005

連邦職員および委託業者の 個人のアイデンティティの検証（PIV：Personal Identity Verification）に関する規格の公布について

FIPS PUB シリーズは、2002 年施行の FISMA の規定に基づき、商務長官の承認を経て NIST により発行される。

1. 規格の名称

FIPS PUB 201：連邦職員および委託業者のアイデンティティの検証

2. 規格の分類

情報セキュリティ

3. 概要

2004 年 8 月 27 日発令の大統領令 HSPD 12『Policy for a Common Identification Standard for Federal Employees and Contractors（連邦職員および委託業者の共通的な身元証明手段の標準に関するポリシー）』では、連邦職員および委託業者を安全かつ高い信頼性で識別する手段について、連邦としての規格を公布するよう命じている。さらに、次の性質を備えた安全かつ高い信頼性の身元証明手段を指定している。

+ 個々の職員のアイデンティティを検証するための確かな基準に基づいて発行されること
+ 身元詐称、アイデンティティの改ざん、偽造、テロリストによる利用に対して強い耐性を有すること
+ 電子的な認証を迅速に行えること
+ 公式の認定プロセスによって信頼性が確立されたプロバイダによってのみ発行されること

この大統領令では、当該規格において最小限の安全性から最大限の安全性までの段階的な基準を設け、用途に応じた適切なレベルのセキュリティを柔軟に選択できるようにすることを定めている。可能な限り迅速に、ただし遅くとも公布当日後 8 か月を超過することなく、執行機関となる省庁および政府機関は、連邦政府の管理下にある施設への物理的アクセスおよび政府の管理下にある情報システムへの論理的アクセスを行う連邦職員および委託業者に対して発行される身元証明について、本規格を実装する必要がある（REQUIRED）。

4. 承認者

商務長官

5. 維持管理機関

商務省、NIST、情報技術ラボラトリ（Information Technology Laboratory、以下 ITL と称す）

6. 適用範囲

本規格は、連邦政府の管理下にある施設への物理的アクセスおよび政府の管理下にある情報システム（合衆国法典第 44 編第 3542 条（b）（2）の定義による「national security systems」（国家安全保障にかかわるシステム）を除く）への論理的アクセスを行うための、連邦政府省庁および政府機関から連邦職員および委託業者（委託業者の従業員を含む）に対して発行される身元証明について適用される。政府機関は、HSPD 12 に規定のある場合を除き、本規格を追加的な用途に使用できるが、このような柔軟性が本規格のいずれかの規定によって変更されることはない。

特定リスクに関するセキュリティ規定—米国政府によって世界各地に配備および運用されている人員、設備、そのほかの資産の中には、極めて広範な脅威（テロリストの脅威、技術的脅威、諜報に関する脅威など）に直面しているものがある。それらの脅威は特に海外において増大している。OCONUS（米国外およびハワイ、アラスカ）で特に注意を要する脅威に直面している機関においては、ここに述べる完全な技術的機能を備えた PIV クレデンシャルを発行、保持もしくは使用することで容認しがたい高リスクを生じる場合がある（MAY）。完全な機能を備えた PIV クレデンシャルが存在すること、および／または使用されることで、顕著なリスク（施設、個人、運用、国益、国家安全保障などに対するもの）が生じる場合、省庁または独立機関の長は、無線機能および／またはバイオメトリック機能を含まない（または部分的にのみサポートする）限りにおいて最大限のセキュリティを備えたクレデンシャルを、特定個数に限って発行することができる（MAY）。省庁または独立機関の長は、政府機関間の相互運用性および大統領のポリシーをサポートする目的で特定リスク対応のクレデンシャルを発行する場合、実際的である限り発行数を最小限にとどめることが望ましい（SHOULD）。そのような状況では、ほかの技術的メカニズム（無線機能の有効・無効を切り替える高い信頼性のスイッチなど）および手続き上のメカニズムをリスク軽減手段として使用することが望ましく、したがってその使用が明示的に許可および推奨される。保護的なセキュリティ技術の進歩に対応するため、本規定に対するこうした必要性は、本規格が通常のレビューおよび更新プロセスの対象となる際に再評価される。

7. 仕様

FIPS 201：連邦職員および委託業者の個人アイデンティティの検証

8. 導入

本 PIV 規格は、PIV-I および PIV-II の 2 部により構成される。PIV-I は HSPD 12 の管理目標およびセキュリティ要件を満たす部分であり、PIV-II は HSPD 12 の技術的相互運用性に関する要件を満たす部分である。PIV-II では、連邦政府機関の個人アイデンティティ検証システムで使用する集積回路チップ内蔵カード式のアイデンティティクレデンシャルに関する実装および使用方法について指定する。

PIV カードを使用して有人および自動化システムの両方によるアイデンティティの検証を行うには、カードに発行対象者固有のアイデンティティを登録する必要がある（MUST）。有人の場合は物理的なカード自体を視覚的に確認することで検証を行う。また、自動化システムの場合はカード上に電子的に格納されたデータを使用して自動的に個人のアイデンティティの検証を行う。

政府の横断的な PIV-II 認定プロセスが確立するまでの間、連邦政府省庁および政府機関は、自らを発行機関として認可するか他の認可済み発行機関を使用することにより、連邦職員および委託業者に対してアイデンティティクレデンシャルを発行できる（MAY）。また、本規格は PIV カードに関するセキュリティおよび相互運用性の要件をも規定する。NIST は財政の許す限り、実装が本規格に適合するかどうかを検証する PIV 認定プログラムの制定を計画している。このプログラムの詳細については、用意できしだいhttp://csrc.nist.gov/npivp/で公開する予定である。

1）発行機関から発行された一般のクレデンシャル、および 2）特定リスクに関するセキュリティ規定に基づいて発行された特定リスク対応のクレデンシャルの各発行数は、行政管理予算局（OMB：Office of Management and Budget、以下 OMB と称す）の定める年次報告プロセスに従って 1 年ごとに OMB に報告されるものとする（SHALL）。

9. 発効日

本規格は直ちに発効する。連邦政府省庁および政府機関は、HSPD 12 の定める日程に従い、PIV-I の要件を 2005 年 10 月 27 日までに満たさなければならない（SHALL）。OMB から NIST への通知によると、OMB では PIV-I から PIV-II への移行に関する手引書の発行を計画している。一部の連邦政府省庁および政府機関では当初から PIV-II を採用する見込みであり、その場合は移行作業が不要になると考えられる（MAY）。

10. 留意事項

PIV システムによって提供されるセキュリティは、本規格の規定に盛り込まれない多数の要素に依拠するものである。本規格を採用するにあたり、各組織では、個人識別システムの全体的なセキュリティが次の事項に依拠することを認識する必要がある（MUST）。

+ クレデンシャルを保有するアイデンティティを正しく確認したことが、当該アイデンティティクレデンシャルの発行機関により保証されること
+ PIV カード内に格納されたアイデンティティクレデンシャル、およびカードと PIV の発行・使用インフラストラクチャとの間で伝送されるアイデンティティクレデンシャルが保護されること
+ 個人アイデンティティ検証システムのインフラストラクチャおよび構成要素が、ライフサイクルのすべての段階を通じて保護されること

本規格の意図は、個人のアイデンティティの検証について高い信頼性を提供するメカニズムと支援システムを示すことであるが、特定の実装が本規格に適合したとしても、その事実によって当該実装の安全性が保証されるものではない。特定の個人アイデンティティ検証システム内で使用される構成要素、インタフェース、通信、格納媒体、管理プロセス、およびサービスについて、設計と構築が安全な形で行われることを保証するのは、当該システム実装者の責任である。

同様に、本規格に適合した製品を使用したとしても、それを使用するシステム全体のセキュリティが保証されるものではない。各省庁および政府機関の責任主体が、システム全体として容認できるレベルのセキュリティが確保されるよう保証しなければならない（SHALL）。

このような性格の規格は科学技術の進歩や革新に対応できる柔軟性を備えていなければならない（MUST）。そのため、NIST では本規格の有効性を評価するレビューを 5 年以内に実施する予定である。NIST では、本規格のフルレビューが必要かどうかについて連邦政府機関からの意見を 1 年以内に募集することを計画している。

11. 適用免除

2002 年施行 FISMA の規定により、FIPS の適用免除は認められない。

12. 規格文書の入手について

本刊行物は、インターネットでhttp://csrc.nist.gov/publications/にアクセスすることにより入手可能である。

目次

付録

図

表

（本ページは意図的に白紙のままとする）

1. はじめに

個人のアイデンティティの認証は、物理的および論理的なアクセス制御プロセスにとって根本をなす要素である。機密性を有する建造物、コンピュータシステム、またはデータに対して個人が何らかのアクセスを試みた場合には、アクセス制御による判断が行われる必要がある（MUST）。アクセス制御において的確な判断を下すには、アイデンティティを正確に把握することが必要とされる。

アイデンティティの認証手段としては、さまざまな種類のアイデンティティクレデンシャルを利用した多様なメカニズムが用いられる。物理的なアクセスについては、アイデンティティの認証は伝統的に、携帯可能な書面あるいはその他の自動化されていない身元証明情報（クレデンシャル）により行われてきた。そのようなクレデンシャルとしては運転免許証やバッジなどがある。コンピュータおよびデータに対するアクセスの伝統的な承認手段としては、ユーザの指定したパスワードによる認証が採用されてきた。最近は暗号メカニズムおよびバイオメトリック技術が、物理的および論理的なセキュリティ用途において伝統的なクレデンシャルを代替または補足する手段として使用されるようになっている。

実現される認証の強度は、クレデンシャルの種類、クレデンシャルの発行プロセス、およびクレデンシャルの検証に使用される認証メカニズムに応じて異なる。本文書は、連邦政府から連邦職員および委託業者に対して発行される安全かつ高い信頼性のある身元識別クレデンシャルに基づくアイデンティティの検証（PIV：Personal Identity Verification）システムに関して一定の標準を確立するものである。それらのクレデンシャルの目的は、連邦政府の管理下にある施設、情報システム、およびアプリケーションに対するアクセスを必要とする個人の認証を行うことである。本規格では、初期段階におけるアイデンティティの立証、アイデンティティクレデンシャルの相互運用性をサポートするインフラストラクチャ、および PIV クレデンシャルの発行機関と発行プロセスに対する認定についての要件を規定する。

1.1 目的

本規格は、連邦政府の管理下にある施設や情報システムへのアクセスなど各種アプリケーションで使用する、政府全体を対象とした信頼性の高い PIV システムを定義するものである。本規格は、連邦法・規制・ポリシーの状況および制約の枠内で、現在利用可能なあるいは発展途上にある情報処理技術に基づいて策定された。

本規格は、共通の個人識別クレデンシャルの作成とそれを使用した身元の検証を実行できる PIV システムを規定する。また、保護の対象となる施設または情報が直面するリスクの程度に応じたセキュリティレベルに関する連邦政府全体の要件を明確にする。

1.2 適用範囲

2004 年 8 月 27 日に大統領署名により成立した、国土安全保障に関する大統領令 12（HSPD：Homeland Security Presidential Directive 12）は、連邦政府の管理下にある施設への物理的アクセスおよび政府の管理下にある情報システムへの論理的アクセスを行う連邦職員および委託業者（委託業者の従業員を含む）に対して発行される身元証明において、共通的に使用される識別手段の標準を確立した。HSPD 12 では、これに基づいた共通的な身元識別クレデンシャルを定義する FIPS PUB シリーズ刊行物の作成を商務省に対して命じている。本規格は HSPD 12 に従い、次の性質を備えたアイデンティティクレデンシャルのための技術的条件を定義するものである。

+ 個々の職員のアイデンティティを検証するための確かな基準に基づいて発行されること

+ 身元詐称、アイデンティティの改ざん、偽造、テロリストによる利用に対して強い耐性を有すること
+ 電子的な認証を迅速に行えること
+ 公式の認定プロセスによって信頼性が確立されたプロバイダによってのみ発行されること

本規格では、異なる強度のセキュリティを提供する認証メカニズムを定義する。連邦政府省庁および政府機関のアプリケーションにおける適切なセキュリティレベルと認証メカニズムは、各省庁および機関が決定する。本規格では、連邦政府省庁および政府機関におけるアクセス制御のポリシーまたは要件については指定しない。したがって、本規格の適用範囲はアイデンティティの認証のみに限定される。アクセス認可の判断については、本規格の規定する対象に含まれない。

1.3 文書の構成

本規格は、PIV-I および PIV-II の 2 部により構成される。第 1 部「PIV-I」では、HSPD 12 の管理目標およびセキュリティ目標に適合する連邦政府機関の個人識別システムに対する最低限の要件を説明する。これにはアイデンティティの立証、登録、および発行に関する要件を含むが、省庁間および政府機関間における PIV カードおよびシステムの相互運用性に関する事項は含まない。

第 2 部「PIV-II」では、PIV-I の管理目標およびセキュリティ目標ならびに連邦政府省庁間および政府機関間における相互運用性をサポートするための詳細な技術仕様を示す。PIV-II では、物理的および論理的アクセスにおける相互運用を可能にする PIV カードのポリシーおよび最低限の要件について説明する。カードの物理的特性、格納媒体、およびアイデンティティクレデンシャルを構成するデータ要素は、本規格において指定する。スマートカードによってアイデンティティクレデンシャルを格納および抽出するためのインタフェースおよびカードアーキテクチャは、NIST SP 800-73（SP 800-73）『個人のアイデンティティの検証インタフェース（Interfaces for Personal Identity Verification）』において指定される。同様に、バイオメトリック情報の収集と表現形式に関する要件は、NIST SP 800-76（SP 800-76）『アイデンティティの検証における生体認証データ仕様（Biometric Data Specification for Personal Identity Verification）』において指定される。

本文書に含まれる各セクションは、*参考情報*（すなわち必須ではない）との明示がある箇所を除き、すべて*標準*（すなわち適合するためには必須）である。本文書の構成は次のとおりである。

+ セクション 1「はじめに」：本規格の適用範囲について理解するための予備知識を示す。このセクションは*参考情報*である。
+ セクション 2「識別、セキュリティ、およびプライバシの共通要件」：HSPD 12 に適合するための管理目標およびセキュリティ目標を明確化することにより、PIV-I の要件の概略を示す。
+ セクション 3「PIV システムの概要」：PIV システムの概要について説明する。このセクションは*参考情報*である。
+ セクション 4「PIV フロントエンドサブシステム」：PIV フロントエンドサブシステムの構成要素に対する要件を示す。具体的には、PIV カード、論理データ要素、バイオメトリクス、暗号技術、およびカードリーダに関する要件を定義する。
+ セクション 5「PIV カードの発行および管理サブシステム」：PIV-II を構成する要素およびプロセスを定義する。また、このサブシステムに関連する要件および仕様について示す。

+ セクション 6「PIV カード認証」: 本セクションでは、PIV カードによりサポートされる各種のアイデンティティ認証メカニズムと、アイデンティティ保証の累進的レベル一式に関する要件を満たす際にそれらのメカニズムを適用できるかどうかについて定義する。
+ 付録 A「PIV プロセス」: アイデンティティの立証および登録、アイデンティティクレデンシャルの発行および管理に関する 2 つのモデルを示す。このセクションは*参考情報*である。
+ 付録 B「PIV の有効性確認、公認、および認定」: 本文書に適合するためのガイダンスを示す。
+ 付録 C「身元調査の詳細」: 身元調査に関する要件を示す。このセクションは参考情報である。
+ 付録 D「PIV オブジェクト識別子」: セクション 4 で定義した各種 PIV オブジェクトについて、より詳細な情報を示す。
+ 付録 E「物理アクセス制御メカニズム」: 物理アクセス制御システム（PACS : Physical Access Control Systems）の保証プロファイルについて説明し、各プロファイルと FIPS 201 の保証レベルとの対応を示す。このセクションは*参考情報*である。
+ 付録 F「用語集および略語集」: 本文書内で使用する語彙の意味および表記を示す。このセクションは*参考情報*である。
+ 付録 G「参考文献」: 本文書内で参照している仕様および規格の一覧を示す。このセクションは*参考情報*である。

第 1 部：PIV-I

この部では、アイデンティティの立証プロセスを含め、HSPD 12 の管理目標およびセキュリティ目標に適合する連邦政府機関のアイデンティティ検証システムに対する最低限の要件を説明する。

履行のタイムフレーム：HSPD 12 に従い、各省庁および政府機関はこの部の要件を、規格の発布から 8 か月以内に満たさなければならない（SHALL）。

2. 識別、セキュリティ、およびプライバシの共通要件

本セクションでは、規格の第 1 部に対する要件を示す。PIV-I は、職員および業務請負企業に対するアイデンティティの立証プロセスを含め、HSPD 12 に概略されている基本的な管理目標およびセキュリティ目標を対象とする。ただし、PIV-I は、PIV クレデンシャルおよびシステムについて連邦政府機関の間の相互運用性を対象とせず、共通利用可能な単独のクレデンシャルの使用を強制するものではない。

2.1 管理目標

[HSPD-12]は、連邦職員および業務請負企業を安全かつ高い信頼性で識別するための管理目標を定めた。大統領指令の第 3 項に記載されている、これらの管理目標を以下に示す:

> (3)この指令における「安全かつ高い信頼性のアイデンティティ」とは、(a)個々の職員のアイデンティティを検証するための確かな基準に基づいて発行され、(b)身元詐称、アイデンティティの改ざん、偽造、テロリストによる利用に対する強い耐性を有し、(c)電子的な認証が迅速に行え、(d)公式の認定プロセスによって信頼性が確立されているプロバイダのみが発行するアイデンティティを意味する。

各政府機関の PIV の実装においては、上記(a)から(d)の管理目標を次のように満たさなければならない(SHALL)。

+ クレデンシャルは、1)本人性が確認された個人に対し、2)クレデンシャルの発行が適切な権限者によって認可された後に発行される。
+ 身元調査の公式記録がある個人に対してのみクレデンシャルが発行される。
+ 個人に対するクレデンシャルは、アイデンティティソース文書を 2 つ提示したあとにのみ発行される。アイデンティティソース文書の少なくとも 1 つは連邦政府または州政府によって発行された写真付きの有効な身分証明書であること。
+ 偽造されたアイデンティティソース文書は、真正かつ改ざんされていないものとして受け付けられない。
+ 政府によってテロリストであると疑われているまたは認識されている個人には、クレデンシャルが発行されない。
+ アイデンティティの立証プロセスにおいてすり替えが起きない。より具体的には、アイデンティティの立証に現れ、その指紋がデータベースと照合される個人が、クレデンシャルの発行対象者本人であること。
+ クレデンシャルは、適切な権限者からの要請のない限り発行されない。
+ クレデンシャルは、有効期限までのみ利用可能である。より具体的には、有効期限切れとなったクレデンシャルおよび失効したクレデンシャルを迅速に無効にできる無効化プロセスが存在すること。
+ プロセスに関与する単独の悪質な職員が、正しくないアイデンティティを持つ身元証明情報を発行したり、クレデンシャルを受け取る資格のない個人にクレデンシャルを発行したりできないこと(MAY NOT)。
+ 発行されたクレデンシャルが変更を加えられたり、複製されたり、偽造されたりしないこと。

2.2 PIVアイデンティティの立証と登録の要件

PIV-I の管理目標に対するコンプライアンスとして、各省庁および政府機関は、アイデンティティクレデンシャルの発行時に以下に規定する要件を満たすアイデンティティの立証と登録のプロセスに従わなければならない（SHALL）。

+ 該当組織は、アイデンティティの立証および登録に関して承認されたプロセスを採用すること（SHALL）。
+ プロセスは、連邦職員の採用時に要求される書面による照会を伴う国家機関身元確認（NACI：National Agency Check with Written Inquiries、以下 NACI と称す）、あるいは人事局（OPM：Office of Personnel Management）または国家安全保障政府機関による他の調査を開始するところから始まるものとする（SHALL）。この要件は、調査が完了し、審査を通過した NACI を特定しそれを参照することによって満たしてもよい（MAY）。最低限、クレデンシャルの発行の前に、FBI 国家犯罪経歴調査（指紋調査）を完了するものとする（SHALL）。第 2 部の開始に当たっては、NACI または同等の調査が完了していない個人に対して発行されたアイデンティティクレデンシャルは、調査が完了した個人に対して発行されたアイデンティティクレデンシャルと電子的に区別できなければならない（MUST）。付録 C「身元調査の詳細」に、国家機関身元確認（NAC：National Agency Check、以下 NAC と称す）および NACI の詳細を示す。
+ PIV クレデンシャルの発行の前に、申請者本人が少なくとも一度は出頭しなければならない（MUST）。
+ アイデンティティの立証中に、申請者はアイデンティティソース文書の原本を 2 種類提示するよう要求されなければならない（SHALL）。アイデンティティソース文書は、「Form I-9, OMB No. 1115-0136, Employment Eligibility Verification（採用適格性検査）」に含まれている受理可能文書一覧に属するものでなければならない（MUST）。文書の少なくとも 1 つは連邦政府または州政府によって発行された写真付きの有効な身分証明書であるものとする（SHALL）。
+ PIV アイデンティティの立証、登録、および発行のプロセスは、特定の個人が、認可された別の個人の協力なしに単独で PIV クレデンシャルを発行できないことを保証する、業務分割の原則に従うこと（SHALL）。

申請者のアイデンティティの検証に用いられるアイデンティティの立証と登録のプロセスは、該当省庁または政府機関によって上記の要件を満たしていることを認定され、連邦政府省庁または政府機関の長の書面による承認がなければならない（SHALL）。これらの要件に適合するプロセスの 2 つの例を付録 A「PIV プロセス」に示す。

これらの要件は、海外で連邦政府のために働いている海外の市民にも適用される。ただし、現地の合衆国軍司令官の指揮下にある従業員を除き、合衆国国務省外交安全保障局によって承認された方法を用いた登録と承認のプロセスを確立しなければならない（MUST）。これらの手続きは、国によって異なることがある（MAY）。

2.3 PIVの発行と維持管理の要件

PIV-I の管理目標に対するコンプライアンスとして、各省庁および政府機関は、アイデンティティクレデンシャルを発行する場合、以下に規定する要件を満たさなければならない（SHALL）。クレデンシャルを発行する場合に用いられる発行プロセス及び維持管理プロセスは、該当省庁によって以下の要件を満たしていることを認定されるとともに、連邦政府の省庁または政府機関の長の書面によ

る承認を受けていなければならない（SHALL）。これらの要件に適合するプロセスの 2 つの例を付録 A に示す。

+ 該当組織は、承認された PIV クレデンシャル発行および維持管理のプロセスを採用すること（SHALL）。

+ プロセスは、連邦職員の採用時に要求される NAC、NACI あるいは人事局（OPM：Office of Personnel Management）または国家安全保障コミュニティによる他の調査の完了と審査の通過を保証するものでなければならない（SHALL）。PIV クレデンシャルは、調査の結果として無効化が妥当と認められた場合には無効にされるものとする（SHALL）。

+ 発行時には、クレデンシャルの発行対象人物（かつ身元調査も完了した人物）が、適切な権限者によって承認された申請者（発行対象者）本人であることを確認すること。

+ 該当組織は、該当機関によって信頼性が確立され、そのように書面にて記録され、承認されている（すなわち、認定されている）システムおよびプロバイダを通じてのみ PIV クレデンシャルを発行するものとする（SHALL）。

2.4 PIVのプライバシ要件

HPSD 12 では、「個人のプライバシを保護すること」が PIV システムの要件の 1 つであることを明示的に規定している。したがって、各省庁および政府機関はすべて、この標準に定められているプライバシ管理策の方針と文言のほか、2002 年電子政府法（E-Government Act of 2002）[E-Gov]、1974 年プライバシ法（Privacy Act of 1974）[PRIVACY]、および行政管理予算局（OMB：Office of Management and Budget）Memorandum M-03-22 [OMB322]に定められている該当する方針と文言に従って PIV システムを実装するものとする（SHALL）。

各省庁および政府機関は、大統領が[HSPD-12]を発行したときに意図もしくは想定していなかった幅広い用途に PIV システムおよびその構成要素を使用することが考えられる（MAY）。PIV システムについて提案されている使用法が適切かどうかを検討するにあたり、各省庁および政府機関は先に述べた管理目標および PIV 標準の目的、特に「セキュリティを強化し、政府の効率を高め、身元詐称を低減し、個人のプライバシを保護する」[HSPD-12]ことを考慮するものとする。各省庁および政府機関は、アイデンティティクレデンシャルについて、これらの管理目標に適合しない使用法を実装してはならない（SHALL）。

申請者のプライバシを保証するために、各省庁および政府機関は以下を行う。（SHALL）：

+ 各政府機関において特定の個人をプライバシ担当の上級職員として任命すること。プライバシ担当の政府機関上級職員は、PIV システムにおけるプライバシ関連事項を監督し、標準に規定されているプライバシ要件を実装する責任を負う。この役割を担う個人は、PIV システムの運用に関して他のいかなる役割も担ってはならない（MAY NOT）。

+ [E-Gov]および[OMB322]に合わせ、PIV の実装を目的として、識別可能な情報形式で個人情報が含まれているシステムを対象にプライバシインパクトアセスメント（PIA）を実施すること。PIV システムを実装する省庁もしくは政府機関においてプライバシ問題について責任を負う適切な職員（最高情報責任者など）に相談すること。

+ 収集する情報（トランザクション情報、識別可能な情報形式[IIF]の個人情報など）、収集の目的、クレデンシャルの存続期間を通じて開示する情報とその開示対象者、情報の保護の方法、および該当省庁または政府機関におけるクレデンシャルと関連情報のすべての使用法を一覧にした明確かつ包括的な文書を記述、公開、および維持管理すること。PIV の申

請者には、PIV クレデンシャルの意図されている用途およびプライバシにかかわる影響について、すべての情報が開示されなければならない（SHALL）。

+ PIV の実装を可能にすることを目的として IIF が格納されているシステムが、[PRIVACY]に規定されている、情報にかかわる公正なプラクティスに全面的に則って扱われることを保証すること。

+ クレデンシャルの発行を拒否されたり無効にされたりした個人が異議申し立てを行う手順を整備すること。

+ PIV システム内の IIF にアクセスする正当な必要性を有する職員のみが、登録とクレデンシャルの発行のために維持管理される情報とデータベースをはじめとする IIF にアクセスすることを認可されるものとする。

+ 適切な省庁または政府機関と協力して、PIV システムのプライバシポリシーに違反した場合の影響を明らかにすること。

+ 各省庁または政府機関における PIV システムの実装で使用されている技術によって、プログラムの運用における情報の収集、使用、配布に関して規定されているプライバシ方針およびプラクティスに従っているかどうかを継続的 に監査することが可能になることを保証すること。

+ プライバシの目的を達成するために、該当する場合、NIST SP 800-53『連邦政府情報システムにおける推奨セキュリティ管理策（Recommended Security Controls for Federal Information Systems）』[SP800-53]で説明しているセキュリティ管理策を利用すること。

+ PIV の実装に使用される技術によって、識別可能な形式での情報の使用、収集、開示に関するプライバシ保護が維持され、侵害されないことを保証すること。具体的には、PIV クレデンシャルに格納されている情報を、許可されていない非接触アクセスから保護するために、電磁的に不透過なカバーまたは他の技術を採用すること。

第 2 部：PIV-II

本文書の第 2 部と、ここで参照されている関連の刊行物では、PIV カードの個人認証とアクセス制御、および連邦政府間の PIV カード管理システムについて、相互運用性の実現に必要な構成要素およびプロセスに関する詳細な技術仕様を説明している。

履行のタイムフレーム：OMB から NIST への通知によると、OMB では、省庁および政府機関における PIV-II への移行計画立案を支援する手引書の発行を計画している。

3. PIVシステムの概要

本セクションでは、以降の各セクションで定義する PIV-II の要件について理解するための予備知識を、概念的な PIV システムアーキテクチャを示しつつ説明する。この PIV システムは、複数種類の物理的および論理的アクセス環境へのアクセスを目的とした、連邦政府省庁間および政府機関の間で共通的に使用される（スマートカードベースの）アイデンティティ認証プラットフォームをサポートする構成要素およびプロセスにより構成される。本規格に示す PIV 構成要素の仕様は、異なる連邦政府省庁および政府機関のシステム間でさまざまな PIV システム構成要素の均質化と相互運用性の実現を促進するものである。本規格に示す各種プロセスの仕様は、運用中の PIV システムにおいて実行する必要があるさまざまの処理に関する最低限の要件セットである。本規格に従って実装した PIV カードは、連邦政府省庁間および政府機関の間で一貫した方法で使用できる一連のアイデンティティ認証メカニズムをサポートする。認証が済んだアイデンティティは、連邦政府の各種物理的および論理的アクセス環境においてアクセス制御の基礎として使用できる。以降の各セクションでは、PIV システムの機能要素と PIV カードのライフサイクル活動について概要を説明する。

3.1 機能要素

運用中の PIV システムは、論理的には、次に示す 3 つのサブシステムに大きく分割できる。

+ **PIV フロントエンドサブシステム**—PIV カード、カードリーダおよびバイオメトリックリーダ、個人識別番号（PIN：Personal Identification Number）入力デバイス。PIV カードの保有者はこれらの要素を操作することにより、目的とする連邦のリソースに対する物理的または論理的アクセスの許可を得る。
+ **PIV カードの発行および管理サブシステム**—アイデンティティの立証と登録、カードと鍵の発行管理、および、検証インフラストラクチャの要素として必要となる各種のリポジトリとサービス（公開鍵基盤（PKI：Public Key Infrastructure）ディレクトリ、証明書状態サーバなど）を担当する構成要素。
+ **アクセス制御サブシステム**—物理的および論理的なアクセスを制御するシステム、保護対象リソース、および承認データ。

アクセス制御サブシステムは、物理的または論理的リソースへのアクセスを求める PIV カード保有者の認証に PIV カードを使用する際に関与する。本規格ではこのサブシステムに関する技術仕様を示さないが、アクセス制御の判断に先立ち認証機能を一貫性と安全性のもとに実行するための各種の識別および認証メカニズムについてセクション 6 で説明する。

図 3-1 は、運用中の PIV システムを表す概念モデルである。各種のシステム構成要素と、それらの間におけるデータフローの方向を図中に示す。

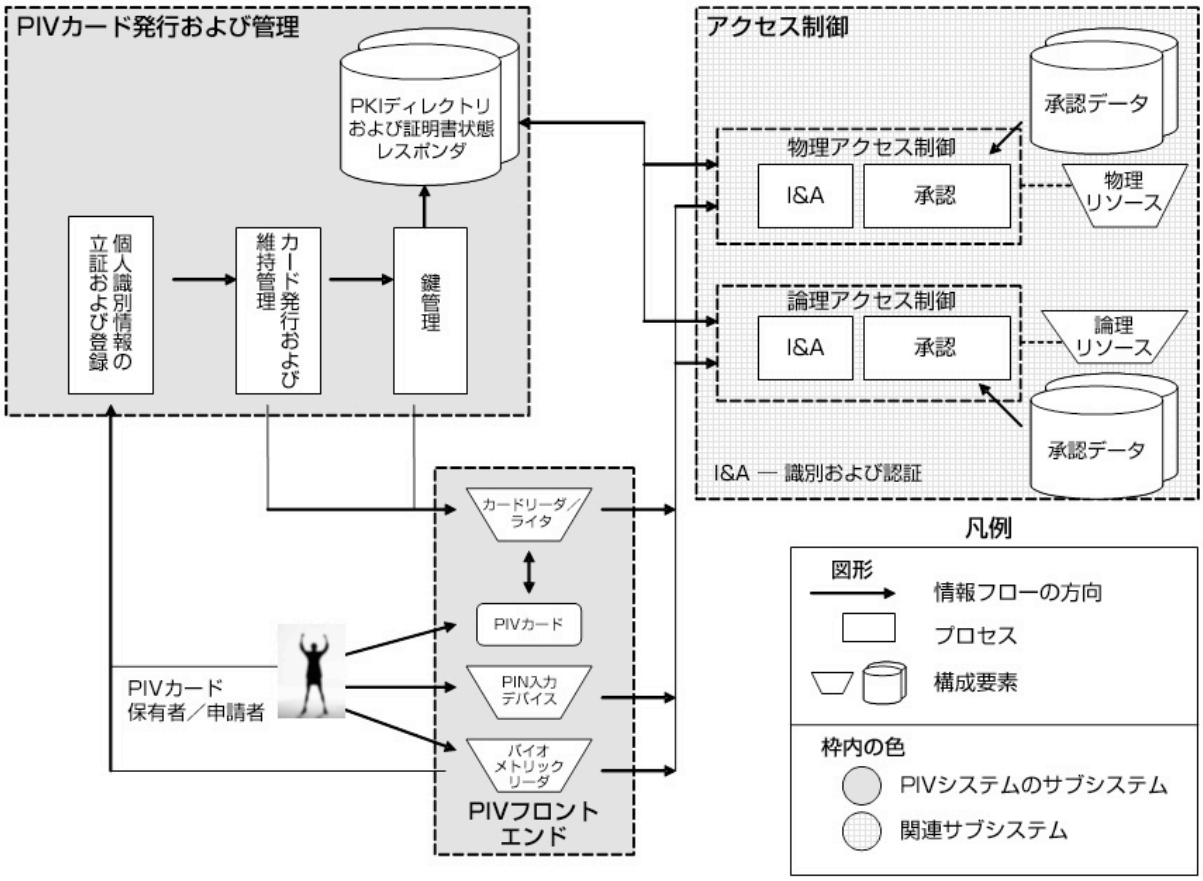


図 3-1. PIV システムの概念モデル

3.1.1 PIVフロントエンドサブシステム

PIV カードは、すべての登録プロセスが完了した後に申請者に対して発行される。PIV カードの形状は、クレジットカード大であり、メモリ領域および計算機能を提供する集積回路チップ（ICC: Integrated Circuit Chip）を 1 つ以上内蔵する。この PIV カードが PIV システムの主要な構成要素である。保有者はさまざまな物理的および論理的リソースに対する認証に PIV カードを使用する。

アクセス制御されたリソースへのアクセス地点にはカードリーダが設置され、カード保有者はそこで必要に応じて PIV カードを使用することによりアクセス（物理的および論理的）の許可を得る。カードリーダは PIV カードと通信し、カードのメモリに格納された適切な情報を取得して、アクセスを許可または拒否するためにアクセス制御システムにその情報を伝達する。

カードライタは、カードリーダとひじょうによく似ているが、PIV カードに格納される情報をパーソナライズし、初期設定する。PIV カードに格納されるデータの内容は、個人情報、証明書、PIN、およびバイオメトリックデータである。これらについては以降の各セクションで詳細に説明する。

カード保有者がアクセスの許可を求めると考えられる地点には、バイオメトリックリーダが設置される場合がある（MAY）。このリーダは、カードのメモリに格納された保有者のバイオメトリックデータを使用し、これをリアルタイムで収集したバイオメトリックサンプルと照合する。バイオメトリックを使

用すると、カードの提示による認証要素(「もっているもの」)にもう 1 つの要因(「持っている特徴」)が加味される。[1]

認証に高いレベルの保証が要求される場合は、カードリーダとともに PIN 入力デバイスも使用されることがある。PIV カードの保有者は、カードを提示する際に PIN 入力デバイスで自分の PIN を入力する必要がある(MUST)。物理的アクセスの場合、PIN の入力は PIN パッドデバイスを通じて行うことが多い。論理的アクセスの場合はキーボードによる入力が一般的である。PIN 入力を使用すると、カード上に保持された情報によるアクセス制御(「持っているもの」)にもう 1 つの認証要素(「知っていること」)が加味され、これによって認証の保証レベルを高めることができる。

3.1.2 PIVカードの発行および管理サブシステム

図 3-1 に含まれるアイデンティティの立証および登録要素は、申請者の身元を確認および保証するために必要なすべての情報と文書に関する収集、格納、維持管理のプロセスを表している。登録時には、さまざまな種類の情報が申請者から収集される。

カードの発行および管理要素は、発行時および以降の維持管理において、カードの物理的側面(表面の外観)および論理的側面(ICC の内容)のパーソナライズ処理に関するものである。これには、写真、名前、その他の情報をカード表面に印刷する処理と、適切なカードアプリケーション、バイオメトリック、その他のデータを格納する処理が含まれる。カード保有者がカードのロックを解除して格納されたクレデンシャルを認証のために提示する能力を制御するために、PIN が使用される。

鍵管理要素は、鍵ペアの生成、カード保有者の公開鍵を含んだディジタル証明書の発行と配布、および証明書状態情報の管理と伝達を担当する。鍵管理要素は、PIV カードのライフサイクルにおけるすべての段階(認証鍵と PKI クレデンシャルの生成および格納から、運用の安全を確保するための鍵使用、カードの更新、再発行および利用停止まで)で使用される。また、PKI クレデンシャルの状態情報を要求元アプリケーションに提供する公開リポジトリおよびサービス(PKI ディレクトリ、証明書状態レスポンダなど)の提供を担当する要素でもある。

3.1.3 アクセス制御サブシステム

アクセス制御サブシステムには、特定の PIV カード保有者が物理的または論理的リソースにアクセスできるかどうかの判断を担当する構成要素が含まれる。物理的リソースとは、カード保有者がアクセスを求める対象となる、セキュリティ保護された施設(建造物の入口、部屋、回転式入出ゲート、駐車場ゲートなど)を意味する。論理的リソースとは、カード保有者がアクセスを求める対象となる、何らかのネットワーク全体またはネットワーク上にある場所(コンピュータワークステーション、フォルダ、ファイル、データベースレコード、ソフトウェアプログラムなど)を意味することが多い。

承認データ要素は、特定の論理的または物理的リソースへのアクセスを求める主体が保有する特権(許可)を定義するための情報を構成する。コンピュータシステム上のファイルに関連付けられるアクセス制御リスト(ACL:Access Control List)はこの一例である。

物理的または論理的アクセス制御システムは、特定リソースへのアクセスを許可または拒否するものであり、識別および認証(I&A:Identification and Authentication)要素と承認要素とを含む。I&A 要素は PIV カードとの通信を行い、セクション 6 で説明するメカニズムを使用してカード保有者を認証する。認証が完了すると、承認要素は承認データ要素と通信し、カード保有者から提示された情報とレコード上の情報とを照合する。アクセス制御要素は、通常の場合、カードリーダ、承認データ、

[1] 「知っていること」、「持っているもの」、「持っている特徴」の詳細については、[SP800-63]を参照。

PIN 入力デバイス、バイオメトリックリーダ、および（利用できる場合は）何らかの証明書状態サービスとのインタフェースを処理するのが普通である。

3.2 PIVカードのライフサイクル活動

PIV カードのライフサイクルは、7 つの活動により構成される。カードの製造、およびパーソナライゼーション前に製造元で行われる処理は、このライフサイクルモデルに含めないものとする。図 3-2 は PIV のライフサイクル活動を示す。このうち最初の活動は PIV カードの申請であり、最後の活動は PIV カードの利用停止である。

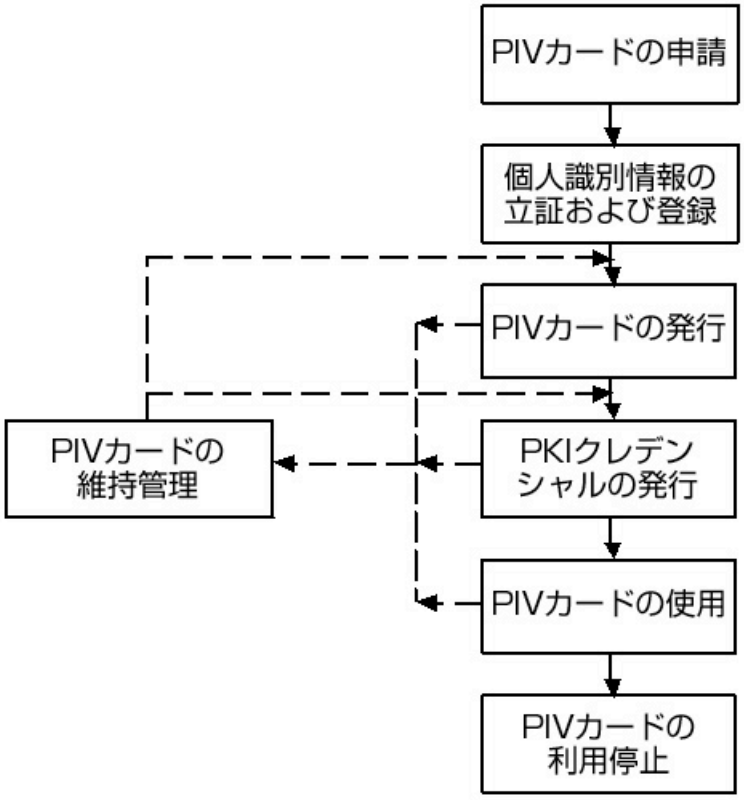


図 3-2. PIV カードのライフサイクル活動

カードのライフサイクルに含まれる 7 つの活動とは次のとおりである。

+ **PIV カードの申請**：この活動は、PIV カードを申請者に発行するよう求める申請書の提出と、その申請に対する有効性確認に該当する。
+ **アイデンティティの立証および登録**：この活動は、申請者から提示された身元証明および登録時に提示されたすべてのアイデンティティソース文書が有効であることの確認を目的とする。
+ **PIV カードの発行**：この活動は、カードの（物理的および論理的）パーソナライズと、そのカードを申請者に対して発行する処理に該当する。
+ **PKI クレデンシャルの発行**：この活動は、論理的なクレデンシャルを生成し、PIV カードに格納する処理に該当する。

+ **PIV カードの使用**:この活動の継続する間、カード保有者による物理的または論理的リソースへのアクセスを認証するために PIV カードが使用される。アクセス承認の判定は、カード保有者の識別および認証が正常に行われた後に下される。
+ **PIV カードの維持管理**:この活動は、物理的なカードおよびそこに格納されたデータの維持管理または更新に該当する。ここでいうデータには、各種のカードアプリケーション、PIN、PKI クレデンシャル、およびバイオメトリックが含まれる。
+ **PIV カードの利用停止**:このプロセスは、PIV カードとその PIV 認証に使用されるデータおよび鍵を永続的に破棄または無効化し、当該カードをそれ以降一切 PIV 認証に使用できなくするために実行される。

4. PIVフロントエンドサブシステム

本セクションでは、PIV フロントエンドサブシステムの構成要素に対する要件を示す。カードの物理的および論理的な仕様については 4.1 項に示す。論理的な PIV カード保有者ユニーク識別子（CHUID：Cardholder Unique Identifier）オブジェクトについてはセクション 4.2 項で説明する。カード保有者に関連付けられる暗号鍵については 4.3 項で説明する。必須のバイオメトリック情報に関するデータ形式の定義は 4.4 項に示す。カードリーダの仕様については 4.5 項で述べる。

4.1 PIVカードの物理的トポロジ

本項および 4.1.1 項から 4.1.4 項において「PIV カード」という場合は、その物理的構造や物理的トポロジに関する特性のみを指す。カードの「表側」という場合は電子的な接点が配置されている面を指し、「裏側」という場合は「表側」の反対の面を指す。

4.1.1 項から 4.1.4 項では、PIV カードの物理的トポロジに関連する情報を示す。PIV カードの物理的トポロジ、外観、その他の特性は、PIV カードが連邦政府における共通の身分証明カードとして認識されることの必要性と、省庁および政府機関ごとに異なる個別の要件をサポートできる柔軟性との両方にバランスよく配慮したものであることが望ましい（SHOULD）。セキュリティおよび相互運用性の向上という目的のために、PIV カードの外観は共通性を備えることが重要である。これらの目的をサポートするには一般に、印刷される要素と技術の配置に一貫性を持たせることが必要となる。

PIV カードは、接触型カードについては国際標準化機構（ISO：International Organization for Standardization）/国際電気標準会議（IEC：International Electrotechnical Commission）の規格 7810 [ISO7810]、ISO/IEC 10373 [ISO10373]、ISO/IEC 7816 [ISO7816]、および非接触カードについては ISO/IEC 14443 [ISO14443]で規定された物理的特性に適合したものとする（SHALL）。

4.1.1 印刷

印刷内容が PIV カードの使用期間中に摩擦で消えることや、印刷およびラミネート処理の工程で塵が侵入することがあってはならない（SHALL NOT）。印刷内容が接触型および非接触 ICC および関連する要素に干渉することや、機械式読み取りが可能な情報へのアクセスを阻害することがあってはならない（SHALL NOT）。

4.1.2 耐改ざん性および耐タンパー性

PIV カードは、偽造防止のために有効な機能を備え、改ざんに対する耐性を有し、改ざんが試みられた場合にその形跡を視覚的に示す能力があるものとする（SHALL）。PIV カードにはこのようなセキュリティ機能を少なくとも 1 つ組み込まなければならない（SHALL）。該当するセキュリティ機能の例を次に示す。

+ 光学的変化材料
+ 光学的変化インキ
+ レーザーエッチングおよびレーザー刻印
+ ホログラム
+ ホログラフィー画像
+ 透かし

セキュリティ機能の組み込みは次の要件に従って行われるものとする（SHALL）。

+ 耐久性要件[ISO7810]に従うこと
+ 劣化や褪色などの欠損が生じないこと
+ 印刷された情報の判読を困難にしないこと
+ 機械式読み取りが可能な情報へのアクセスを阻害しないこと

省庁および政府機関は、必要に応じて追加的な耐タンパー性および偽造対策を導入してよい（MAY）。連邦政府省庁および政府機関には一般的なセキュリティ手順として、採用された改ざん防止策および偽造対策の実現性、実効性、通用性を精査することを強く推奨する。

4.1.3 物理的特性および耐久性

PIV カードにおける物理的要件の一覧を次に示す。

+ PIV カードは、接触型および非接触 ICC インタフェースを備えるものとする（SHALL）。
+ カード本体の構造は、[ISO7810]で規定されるカードの特性および米国国家規格協会（ANSI：American National Standards Institute）の規格 322 [ANSI322]で規定されるテスト方法を満たす材料によるものとする（SHALL）。現在、[ANSI322]のテスト方法には適合要件が指定されていないが、カード材料の耐久性および性能の評価にはこのテストを使用するものとする（SHALL）。[ANSI322]テストの内容としては、少なくとも、カードの屈曲、静的応力、可塑剤暴露、耐衝撃性、カード構造上の保全性、表面の摩耗、温度および湿度による色移り、紫外線暴露、洗濯テストを含めるものとする（SHALL）。通常の石鹸と水との混合液でカードを手洗いした場合に機能不全または剥離を生じてはならない（SHALL NOT）。[ISO10373]の 5.4.1.1 項に挙げられている試薬に、石鹸 2 パーセント水溶液も含めるものとする（SHALL）。
+ [ISO10373]の 5.12 項に従い、自然の太陽光、集中させた太陽光、または人工の太陽光を使用して、米国南西部の太陽光による 2000 時間の暴露による影響を正しく反映した暴露テストを実施するものとする（SHALL）。集中させた太陽光による暴露の場合は[G90-98]に従って、また、促進暴露の場合は[G155-00]に従って行うものとする（SHALL）。暴露後のカードに対して[ISO10373]の動的屈曲テストを実施し、その結果として視認可能な割れまたは破損が生じてはならない（SHALL NOT）。または代替テストとして、[ANSI322]に基づく紫外線および太陽光での耐褪色性テストの後に同じく[ISO10373]の動的屈曲テストを実施してもよい（MAY）。

PIV カードに対しては必要に応じて追加的なテストを実施してよい（MAY）。

+ カードの厚さは、[ISO7810]に従い 27 ないし 33 ミル（ラミネート加工を含まず）とする（SHALL）。
+ PIV カードにエンボス加工を施してはならない（SHALL NOT）。
+ PIV カードに転写ステッカーを貼付してはならない（SHALL NOT）。
+ 省庁および政府機関の裁量により、カード本体には紐通し穴を 1 個穿孔することができる（MAY）。このような改変を加える場合、省庁および政府機関は、カード材料の保全性に悪影響を及ぼさないようカードのベンダーまたは製造元との調整を密にすることが望ましい

（SHOULD）。省庁および政府機関には、このような改変にあたって次の問題に対する確実な防止策を講じるよう強く推奨する。

- カード本体の耐久性および特性の減退
- カード製造元の保証、その他製品に関する権利の無効化
- 印刷された情報（写真を含む）に対する改変または干渉
- 機械式読み取り技術（内蔵アンテナなど）に対する損傷または干渉

カードに物理的改変を加えることなく装着を可能にする代替手段として、市販されている各種カードホルダおよびカードキャリアの使用が考えられる。カードへの物理的な穿孔を避け、カードキャリアを使用することを推奨する（RECOMMENDED）。

+ カード材料は、市販の既製品（COTS：Commercial Off-The-Shelf）機器を使用してカード片面または両面にポリエステルラミネート加工を施す場合に必要となる加熱処理に耐えるものとする（SHALL）。ラミネート層による厚さの増加は、スマートカードリーダの運用を阻害してはならない（SHALL NOT）。カード材料は、カードの片面または両面にラミネート加工を施した後で[ISO7810]に基づく平坦なカードを作成可能なものとする（SHALL）。

4.1.4 カードの視覚的な要素配置

PIV カード上の情報は、視覚的な印刷および電子的な形態で格納されるものとする（SHALL）。本項では視覚情報および印刷される情報について説明する。データ要素など電子的形態で格納される情報と、その他使用される可能性がある機械式読み取り技術についてはここで扱わない。論理的に格納されるデータ要素については 4.1.5 項で述べる。

4.1.3 項で述べたとおり、PIV カードは接触型および非接触 ICC インタフェースを備えるものとする（SHALL）。本規格では、必須である接触型および非接触インタフェースをサポートするために使用するチップの数を単一とするか、複数とするかについては指定しない。

PIV カードの外観の共通性を維持しつつ、各省庁および政府機関ごとの特有の要件に基づいてカードを強化できる柔軟性をも提供するため、カードは必須および任意の印刷情報と、必須および任意（OPTIONAL）の機械式読み取り技術とを備えるものとする（SHALL）。必須および任意（OPTIONAL）の項目は、おおむね説明および図示する通りに配置されるものとする（SHALL）。印刷されるデータは機械式読み取り技術と干渉してはならない（SHALL NOT）。

予約済みと表示した領域を印刷に使用することは望ましくない（SHOULD NOT）。推奨予約済み領域を規定する理由は、内蔵される非接触 ICC モジュールの配置が製造元によって異なる場合があることから、内蔵される非接触 ICC モジュールの位置に印刷が重なることを防ぐための制約も一定でないためである。PIV カードトポロジの規定では、埋め込みモジュールの位置に柔軟性を認めており、右上隅または下端部のいずれかが許容される。印刷の制限は、埋め込みモジュールが配置される領域（右上隅または下端部）にのみ適用される。

技術の発展により、制限領域を設ける必要性がなくなるか制限領域のサイズが変化する可能性があるため、省庁および政府機関はカードベンダーおよび製造元との連携を密にし、最新の印刷手順および印刷方法を確実に適用するとともに、PIV カードの耐タンパー性と偽造防止能力とを向上する機能の組み込みの可能性について検討することを推奨する。

4.1.4.1 PIVカード表側の必須項目

*ゾーン1—写真:*図 4-1 に示すとおり、写真は左上隅に配置し、頭部から肩までを真正面から写したものとする（SHALL）。画像の解像度は 300 ドット／インチ（dpi）以上とする（SHALL）。背景については、SP 800-76 に規定された推奨事項に従うことが望ましい（SHOULD）。

*ゾーン2—氏名:*フルネーム [2]を写真のすぐ下に、大文字で印刷するものとする（SHALL）。フォントのサイズは 10 ポイント以上とする（SHALL）。

*ゾーン8—職員の身分:*職員の身分をカード上に印刷するものとする（SHALL）。身分の例としては「CONTRACTOR」（委託業者）、「ACTIVE DUTY」（現役）、「CIVILIAN」（民間人）などがある。

*ゾーン10—所属組織:*図 4-1 に示すとおり所属組織を印刷するものとする（SHALL）。

*ゾーン14—有効期限:*カードの有効期限を「YYYYMMMDD」形式で印刷するものとする（SHALL）。

4.1.4.2 PIVカード裏側の必須項目

*ゾーン1—連邦政府機関カードシリアル番号:*この項目は図 4-6に示すとおり印刷するものとする（SHALL）（本文書末尾の変更告知に記載した重要事項を参照）。発行元である省庁または政府機関により発番される固有のシリアル番号を示す。形式は、発行元である省庁または政府機関の裁量によるものとする（SHALL）。

*ゾーン2—発行元識別情報:*この項目は図 4-6に示すとおり印刷するものとする（SHALL）（本文書末尾の変更告知に記載した重要事項を参照）。6 字の省庁コード、4 字の機関コード、および、該当省庁または政府機関内の発行元施設を一意に識別する 5 桁の数字を示す。

4.1.4.3 カード表側の任意使用項目

本項では、任意（OPTIONAL）で表示可能な情報および任意で使用可能な機械式読み取り技術と、これらの配置について説明する。任意で使用可能な技術に関する格納容量は、各省庁および政府機関の規定によるものとし、本規格には規定しない。本項で説明する項目は任意使用項目であるが、使用する場合のカード上への配置については例および注記に従うこと（SHALL）。

*ゾーン3—署名:*使用する場合、該当省庁または政府機関は図 4-3 に示すとおり、カード保有者の署名を写真および保有者氏名の下に表示するものとする（SHALL）。署名用の領域は接触型および非接触 ICC に干渉してはならない（SHALL NOT）。カード上のスペースの制約により、署名を表示する場合は任意使用の 2 次元バーコードのサイズに制限が生じることがある（MAY）。

*ゾーン4—該当政府機関に特有のテキスト領域:*使用する場合、該当政府機関に特有の要件による項目（雇用形態など）をこの領域に印刷できる。

*ゾーン5—階級:*使用する場合、カード保有者の階級を図に示すとおり印刷するものとする（SHALL）。データ形式は、該当省庁または政府機関の裁量による。

*ゾーン6—可搬データファイル（PDF :Portable Data File）形式の 2 次元バーコード:*使用する場合、PDF バーコードを図に示すとおり（カード左端に）表示するものとする（SHALL）。ゾーン 3（カード保有者の署名）を使用する場合、PDF バーコードのサイズに制限が生じることがある（MAY）。カード

[2] もしくは法に基づいて使用される通称。

保有者の署名を表示するPIVカードにPDFも表示する場合、カード発行者は、PDFに期待されるデータ格納要件が満たされるかどうか確認することが望ましい（SHOULD）。

*ゾーン9— ヘッダ:*使用する場合、「*United States Government*」（合衆国政府）というテキストを図4-1に示すとおり表示するものとする（SHALL）。または、省庁および政府機関の裁量により、省庁および政府機関に特有のほかの情報をこの領域に表示してもよい（MAY）。たとえば、図4-2に示すように連邦政府緊急時対応要員の任務を示すことが考えられる。

*ゾーン11—政府機関の印章:*使用する場合、発行元である省庁、政府機関、その他の組織により指定された印章を図に示すとおり印刷するものとする（SHALL）。図 4-2 に示すガイドラインに従い、印章の上に印刷される情報は明瞭かつ容易に判読可能でなければならない（SHALL）。

*ゾーン12—フッタ:*フッタは、*緊急時対応要員の識別*ラベルを表示する場合の推奨位置である。使用する場合は、「Federal Emergency Response Official」（連邦政府緊急時対応要員）というテキストを図4-2に示すとおり表示してよい（MAY）。テキストの色は赤が望ましい。省庁および政府機関の裁量により、緊急時対応要員の正規の任務をより具体的に示す追加的なテキスト行をゾーン9に表示してよい（MAY）。任務の例としては「Law Enforcement」（法執行官）、「Firefighter」（消防士）、「Emergency Response Team (ERT)」（緊急事態対応チーム）などがある。

*ゾーン13—発行日:*使用する場合、図4-2に示すとおり、有効期限の上にカードの発行日を「YYYYMMMDD」形式で印刷するものとする（SHALL）。

*ゾーン15—身分識別用のカラーコーディング:*職員の身分を識別しやすくするために、カラーコーディングの利用を追加してよい（MAY）。カラーコーディングを使用する場合、図4-4に示すとおりゾーン2（氏名）の背景色として表示するものとする（SHALL）。次の分類については所定の色分けに従うこと（SHALL）。

+ 青—外国人
+ 赤—緊急時対応要員
+ 緑—委託業者

これらは予約済みの色とし（SHALL）、他の用途に使用してはならない（SHALL NOT）。ゾーン15の色は、該当省庁または政府機関の裁量により、べた塗りまたは網掛けのいずれかの方法で表示してよい（MAY）。

*ゾーン16—身分識別用の写真縁取り線:*職員の身分を識別しやすくするために、図4-3に示すとおり写真の周囲に縁取り線を追加してよい（MAY）。省庁および政府機関は、この縁取り線をゾーン15と組み合わせ、職員をさまざまに分類する手段として使用できる（MAY）。縁取り線は写真の視認を妨げてはならない（SHALL NOT）。縁取り線の形状としては実線またはパターン線を使用できる（MAY）。実線およびパターン線とも、赤は緊急時対応要員、青は外国人、緑は委託業者の識別用に予約済みの色とする（SHALL）。その他すべての色は、該当省庁または政府機関の裁量により使用してよい（MAY）。

*ゾーン17—該当政府機関に特有のデータ:*これ以外の任意使用要素を使用しない場合、図4-5に示すとおり、ゾーン17を使用して該当政府機関に特有のほかの情報を表示できる（MAY）。

4.1.4.4 カード裏側の任意使用項目

*ゾーン 3—磁気ストライプ:*使用する場合、磁気ストライプは高い保磁力を有するものとし、図 4-7 に示すとおり[ISO7811]に従って配置するものとする（SHALL）。

*ゾーン 4—遺失物の送付先:*使用する場合、カード裏側には、遺失時の発見者に返送を求める文言をおおむね図 4-7 に示すとおり表示するものとする（SHALL）。

*ゾーン 5—カード保有者の身体的特徴:*使用する場合、カード保有者の身体的特徴（身長、瞳の色、髪の色など）をおおむね図 4-7 に示す領域に印刷するものとする（SHALL）。

*ゾーン 6—緊急時対応要員に関する追加的な文言:*省庁および政府機関の裁量により、緊急時対応要員に関する追加的な情報、またはカード保有者が認可されたアクセス対象をより明確に示すための追加的な情報を表示できる（MAY）。使用する場合、この追加的なテキストはおおむね図に示す領域に表示するものとする（SHALL）。ただし、これがほかの印刷されるテキストまたは機械式読み取り可能な要素に干渉してはならない（SHALL NOT）。印刷する文言の例を図 4-7 に示す。

*ゾーン 7—合衆国法典第 18 編第 499 条の規定による文言:*使用する場合、おおむね図 4-7 に示す領域に、合衆国法典第 18 編第 499 条に基づくカードの偽造、改変、濫用に対する警告の文言を印刷するものとする（SHALL）。

*ゾーン 8—Code 39 一次元バーコード:*使用する場合、Code 39 一次元バーコードをおおむね図 4-7 に示す位置に表示するものとする（SHALL）。形式は自動認識モビリティ協会（AIM : Association for Automatic Identification and Mobility）の規格に従うものとする（SHALL）。バーコードの開始位置および終了位置は、内蔵する非接触モジュールの選定に応じて異なる。省庁および政府機関はバーコードの配置についてカードベンダーと調整することを推奨する。

*ゾーン 9—該当政府機関に特有のテキスト:*これ以外の任意使用要素を使用しない場合、図 4-8に示すとおり、ゾーン 9 を使用して該当政府機関に特有の他の情報を表示できる（MAY）（本文書末尾の変更告知に記載した重要事項を参照）。たとえば、緊急時対応要員に関する追加的な詳細事項を示すためにこの領域を使用することが考えられる（MAY）。

*ゾーン 10—該当政府機関に特有のテキスト:*ゾーン 10 はゾーン 9 と同様、該当政府機関に特有の情報を表示する目的に使用できる。

省庁および政府機関には、ゾーン 9 および 10 について、これらの領域の使用に慎重であること、印刷内容を最低限必要な事項のみに限定することを推奨する。

国防総省の場合、カード裏側は独特の外観を備えるものとする。本規定は、Geneva Accord（ジュネーブ合意）により要求される情報を表示するため、および法律上必須とされる医療処置の権利に関する便宜のために必要である。

- 周囲の寸法表示はミリ単位、左上隅からの長さ。
- すべてのテキストは Arial フォントで印刷。
- 特記なき場合の推奨フォント ― データラベル（タグ）：5ポイント、太さ標準。実際のデータ：6ポイント、太字。

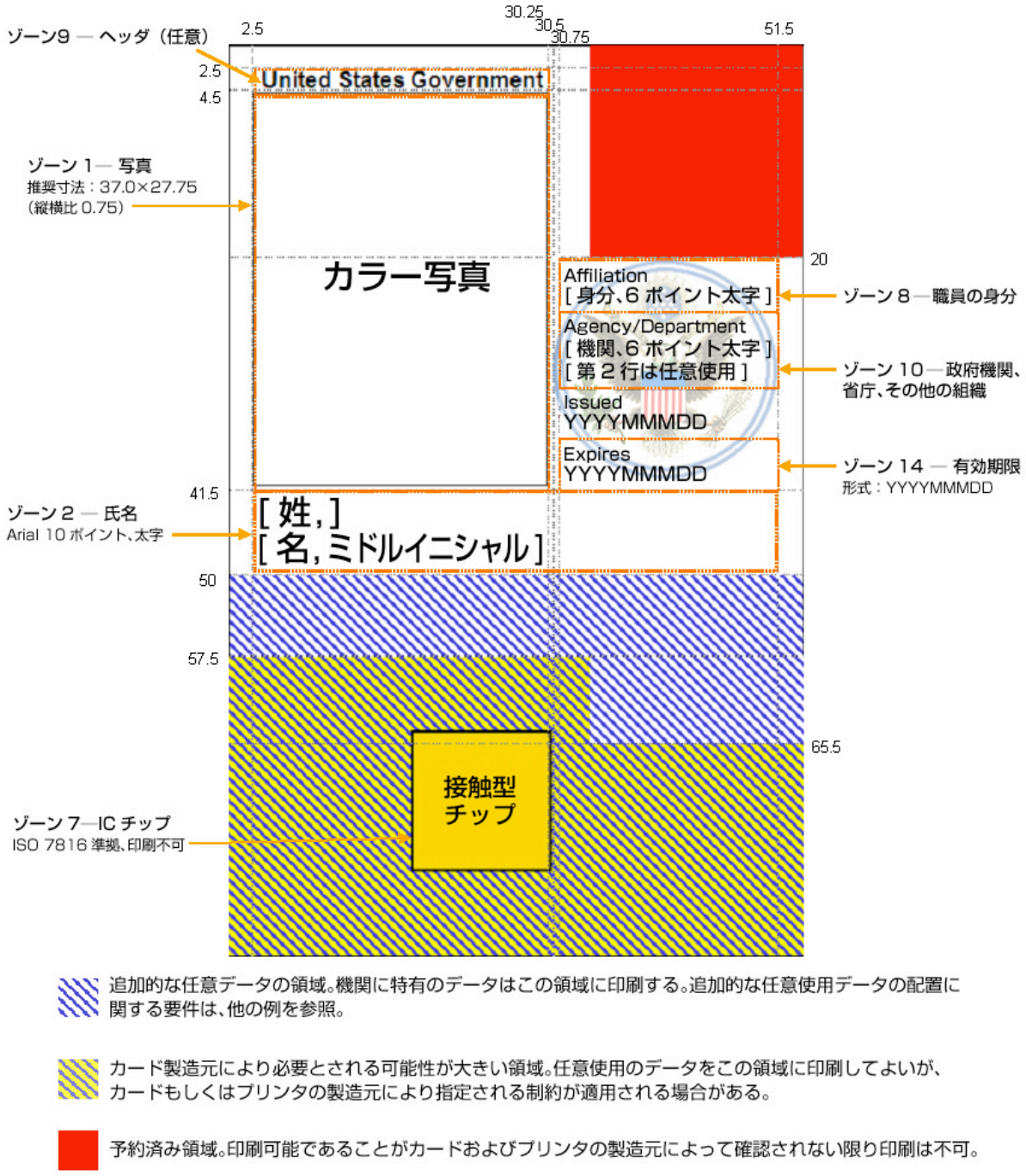


図 4-1. カード表側―印刷に使用可能な領域

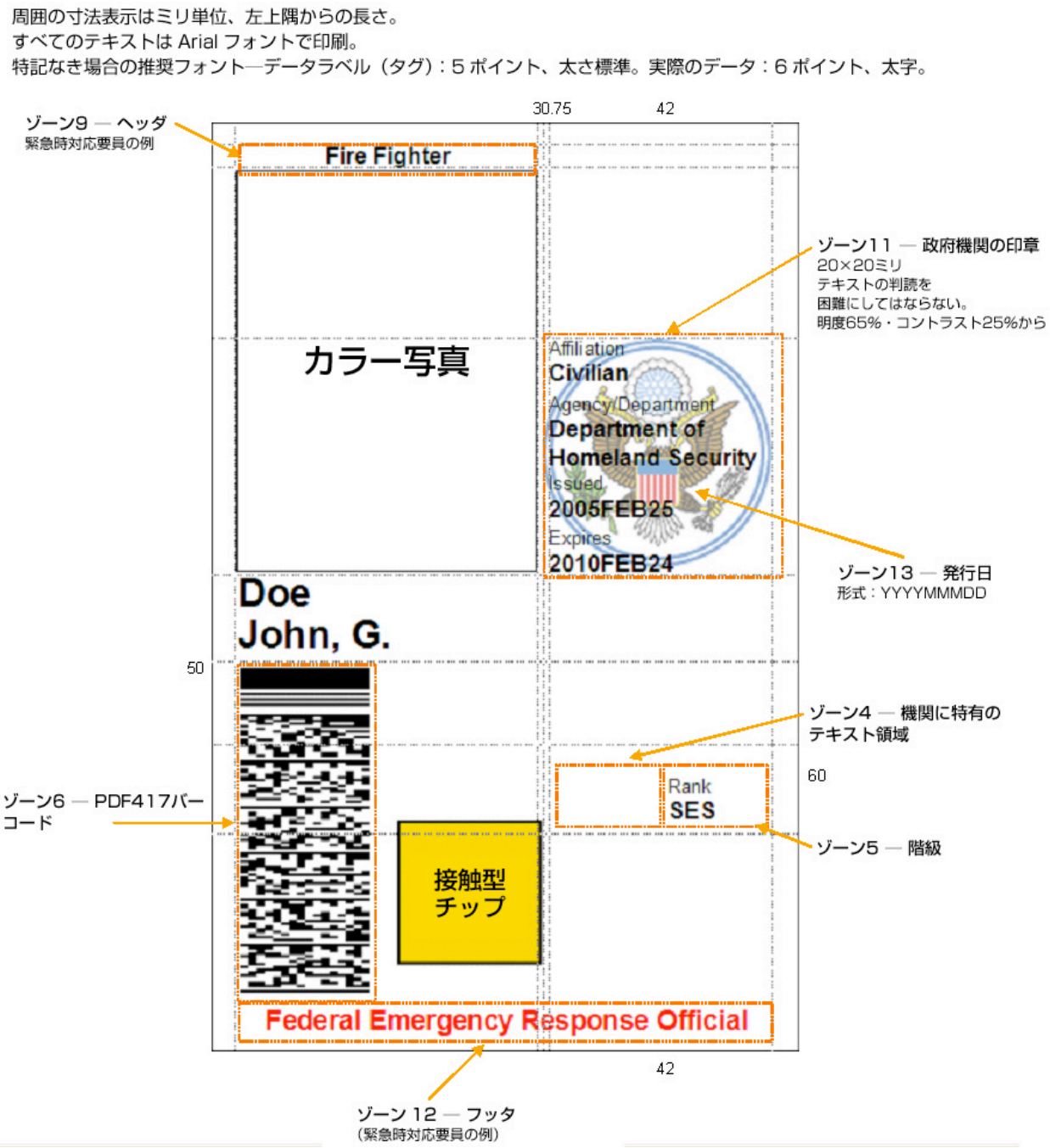


図 4-2. カード表側—任意使用データの配置—例 1

周囲の寸法表示はミリ単位、左上隅からの長さ。
すべてのテキストは Arial フォントで印刷。
特記なき場合の推奨フォント―データラベル（タグ）：5 ポイント、太さ標準。
実際のデータ：6 ポイント、太字。

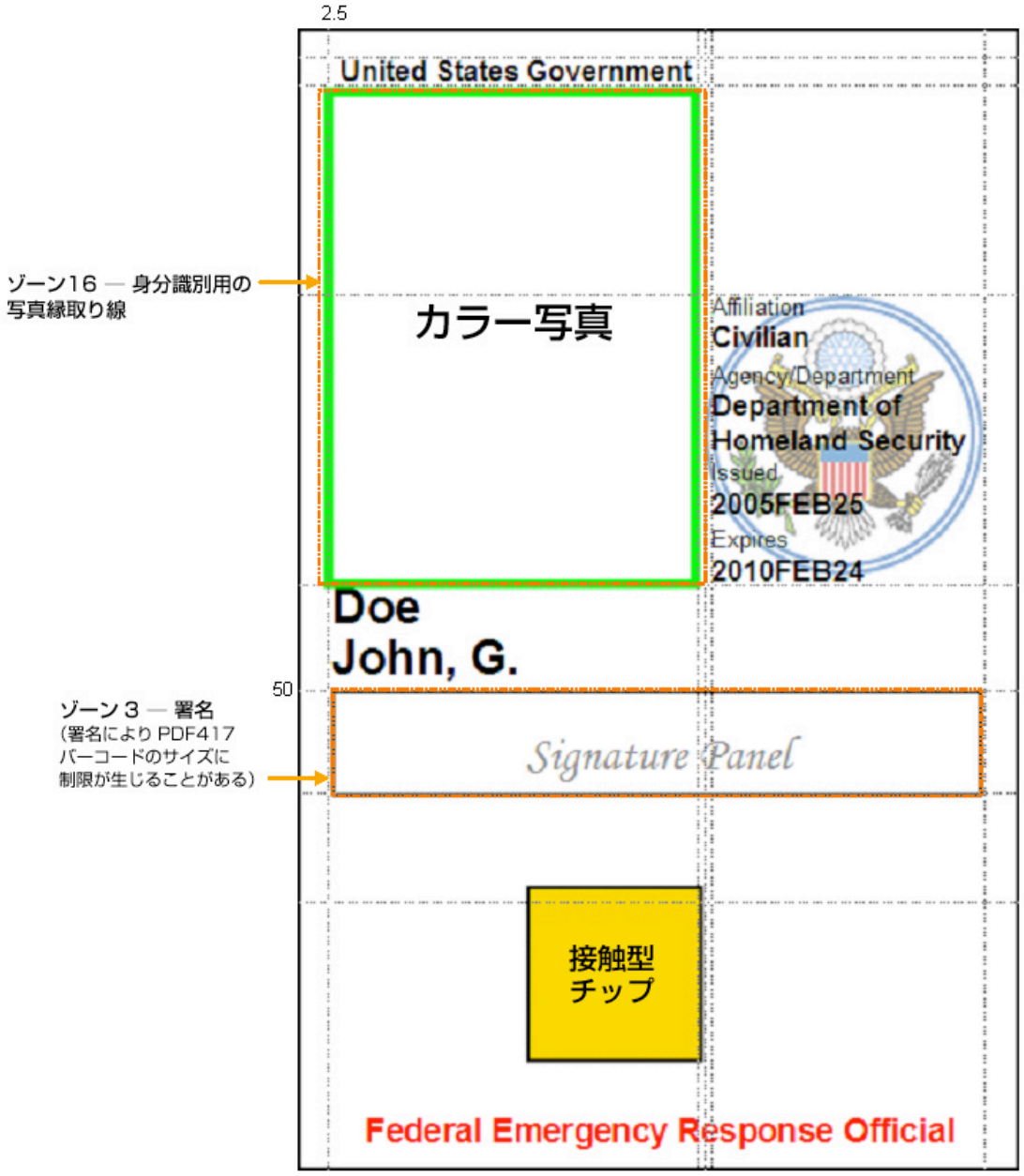


図 4-3. カード表側―任意使用データの配置―例 2

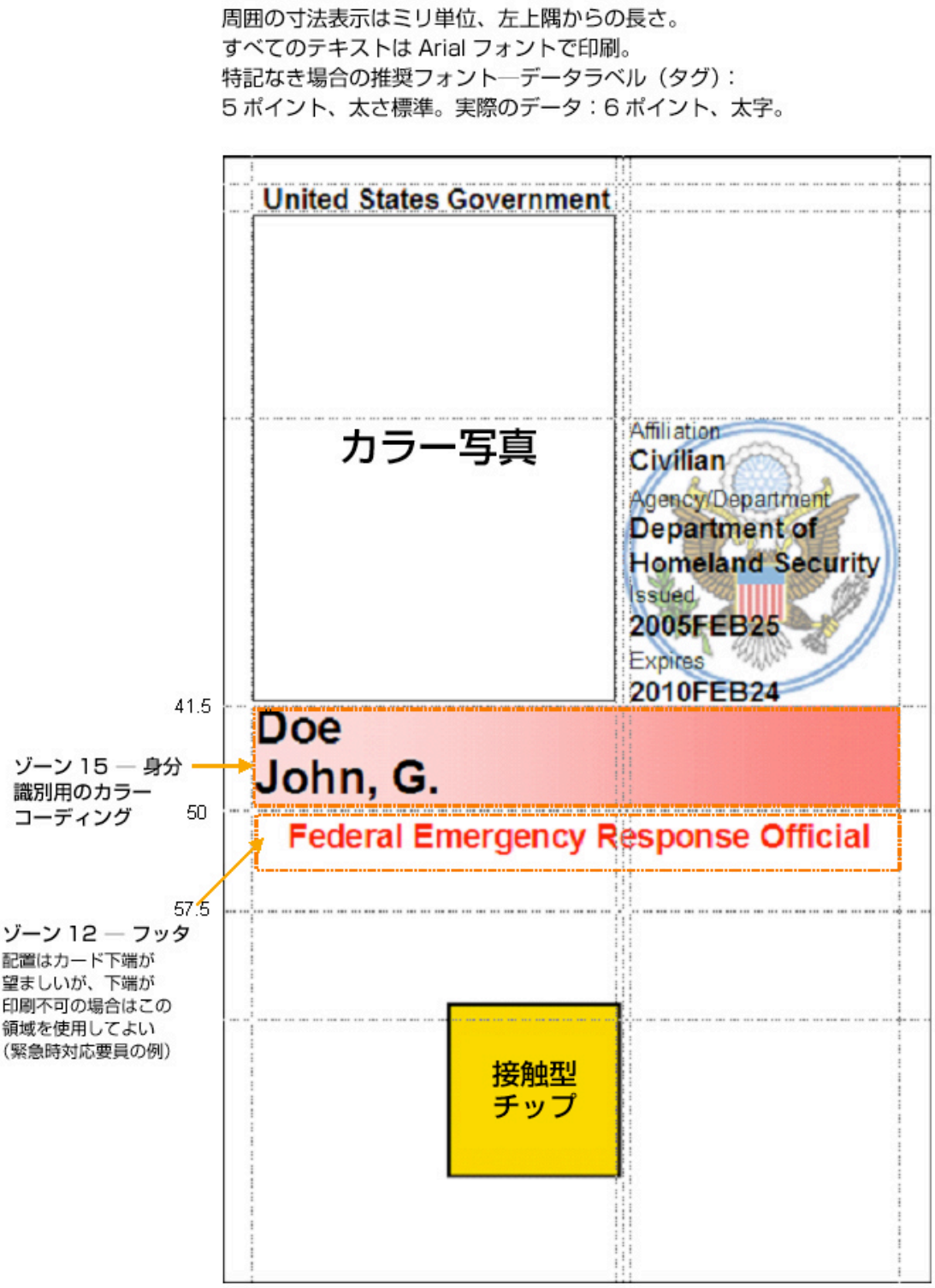
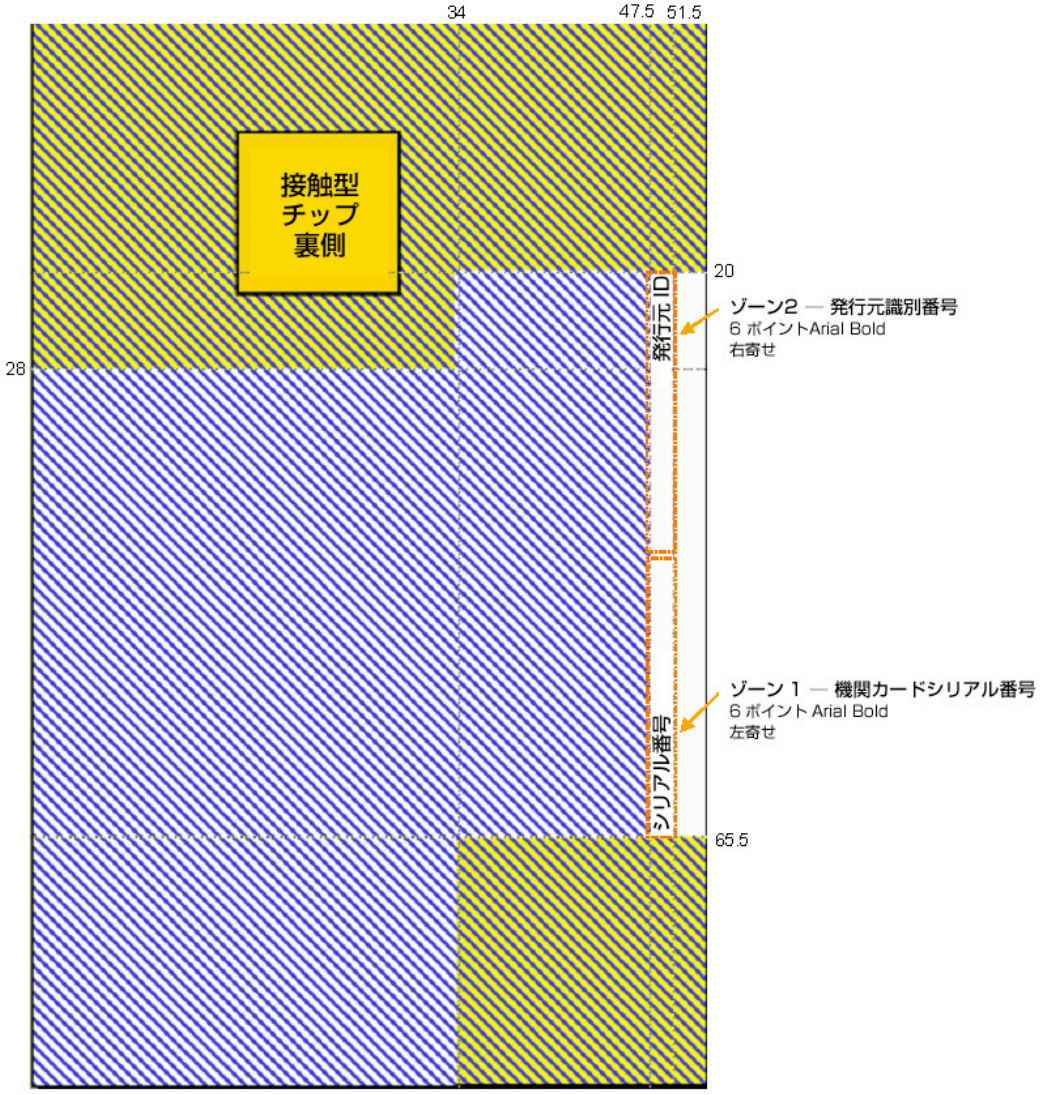


図 4-4. カード表側—任意使用データの配置—例 3

周囲の寸法表示はミリ単位、左上隅からの長さ。
すべてのテキストはArialフォントで印刷。
特記なき場合の推奨フォント — データラベル（タグ）：5ポイント、太さ標準。実際のデータ：6ポイント、太字。

図 4-5. カード表側—任意使用データの配置—例 4

周囲の寸法表示はミリ単位、左上隅からの長さ。
すべてのテキストは Arial フォントで印刷。
特記なき場合の推奨フォント—データラベル（タグ）：5 ポイント、太さ標準。実際のデータ：6 ポイント、太字。



任意データの領域。機関に特有のデータはこの領域に印刷する。追加的な任意使用データの配置に関する要件は、例を参照。

カード製造元により必要とされる可能性が大きい領域。任意使用のデータをこの領域に印刷してよいが、カードもしくはプリンタの製造元により指定される制約が適用される場合がある。

図 4-6. カード裏側—印刷に使用可能な領域および必須データ

周囲の寸法表示はミリ単位、左上隅からの長さ。
すべてのテキストは Arial フォントで印刷。
特記なき場合の推奨フォント — データラベル（タグ）：5 ポイント、太さ標準。実際のデータ：6 ポイント、太字。

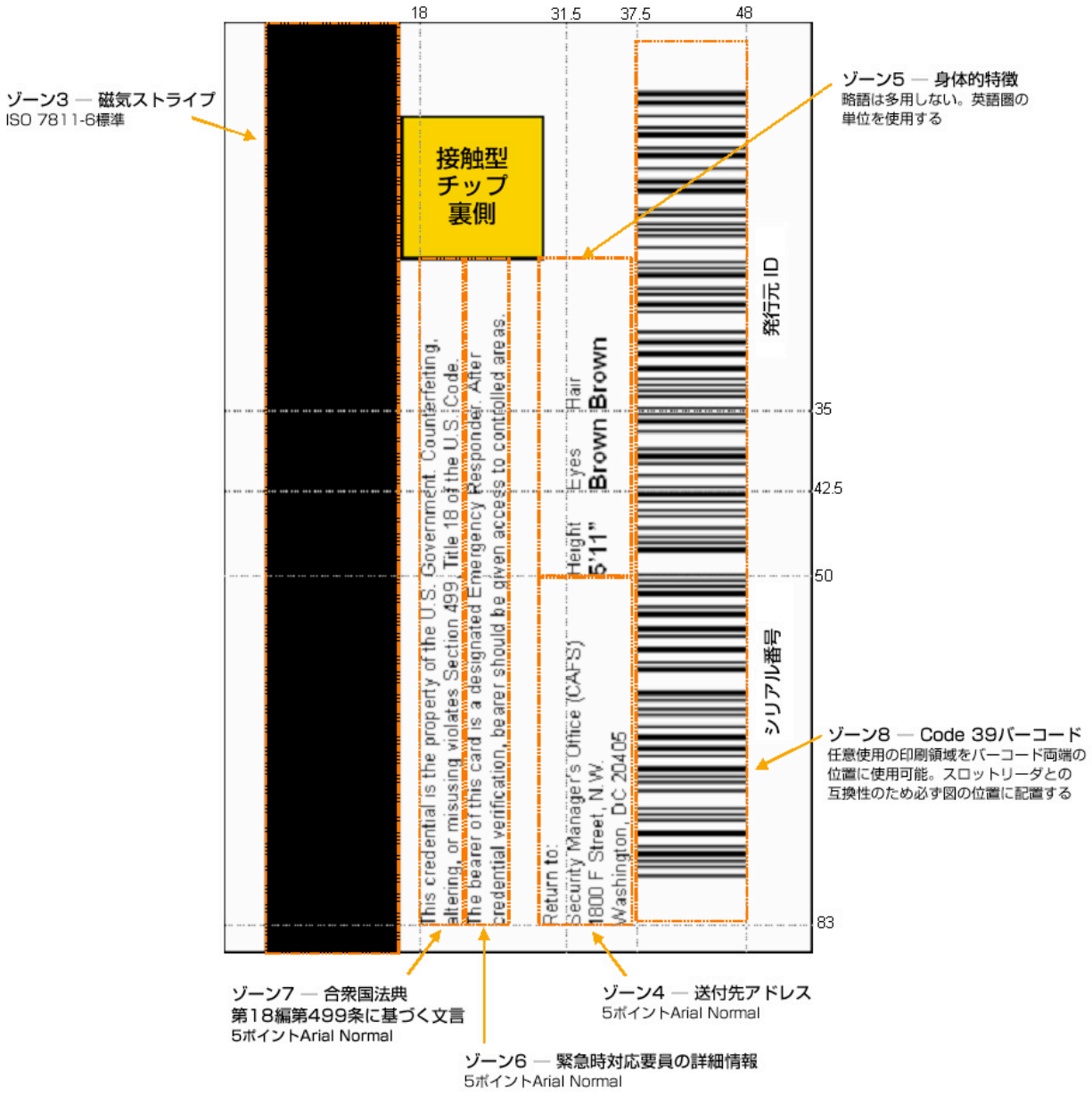


図 4-7. カード裏側—任意使用データの配置—例 1

周囲の寸法表示はミリ単位、左上隅からの長さ。
すべてのテキストは Arial フォントで印刷。
特記なき場合の推奨フォント—データラベル（タグ）：5 ポイント、太さ標準。実際のデータ：6 ポイント、太字。

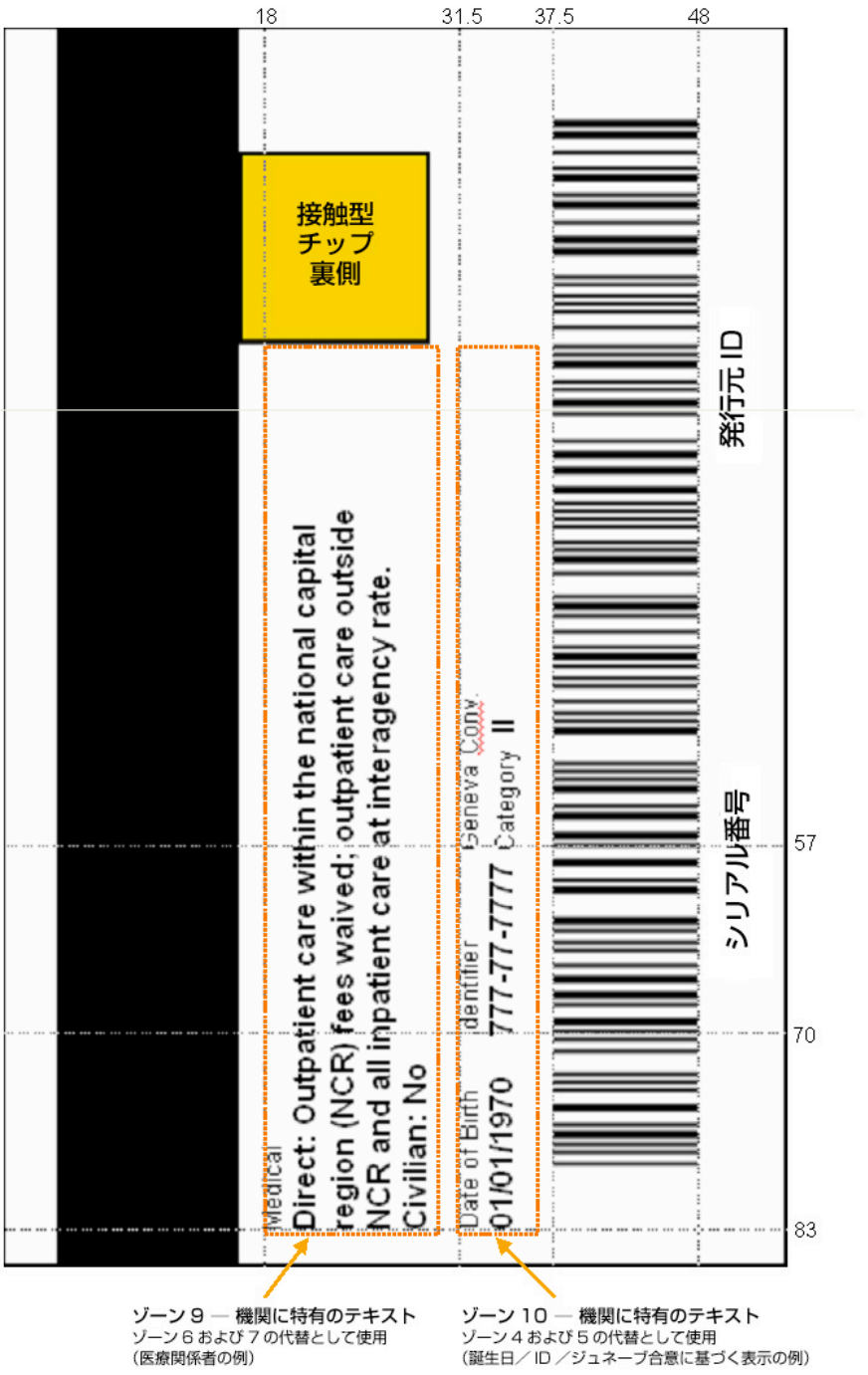


図 4-8. カード裏側—任意使用データの配置—例 2

4.1.5 論理クレデンシャル

本項では、論理的なアイデンティティクレデンシャル、およびその使用に関する要件について定義する。具体的には、アイデンティティクレデンシャルの構成および活性化の詳細について説明する。

4.1.5.1 論理クレデンシャルデータモデル

さまざまな認証メカニズムをサポートするため、PIV の論理クレデンシャルは、段階的に異なる各種の保証レベルにおいてカード保有者アイデンティティの検証に使用する複数のデータ要素を含むものとする（SHALL）。それらの必須データ要素が、総体として PIV 論理クレデンシャルのデータモデルを構成する。含まれる要素は次のとおりである。

+ PIN
+ CHUID
+ PIV 認証データ（一組の非対称鍵ペア、およびそれに対応する証明書）
+ 2 個のバイオメトリック指紋

PIV データモデルは、各省庁または政府機関に特有の要件に応じて拡張することもできる（MAY）。データモデルを拡張する場合について、本規格では次の 4 クラスの論理クレデンシャルに関する要件を規定する。

+ ディジタル署名に使用する一組の非対称鍵ペアおよびそれに対応する証明書
+ 鍵管理に使用する一組の非対称鍵ペアおよびそれに対応する証明書
+ 追加的な物理アクセス用途をサポートするために使用する非対称または対称のカード認証鍵
+ カード管理システムに関連付けられる対称鍵

PIV の論理クレデンシャルは、次の 3 種別に分類される。

1. カードに対してカード保有者の本人性を証明するためのクレデンシャル要素（CTC 認証）
2. カードに対してカード管理システムのアイデンティティを証明するためのクレデンシャル要素（CMTC 認証）
3. カードが外部の主体（ホストコンピュータシステムなど）に対してカード保有者の本人性を証明するためのクレデンシャル要素（CTE 認証）

PIN は第 1 の種別に、カード管理鍵は第 2 の種別に、また、CHUID、バイオメトリック情報、対称鍵、非対称鍵は第 3 の種別に分類される。

4.1.6 PIVカードの活性化

バイオメトリック情報の読み出しや非対称鍵の使用など特権操作 [3]を実行するには、PIVカードを活性化 [4]する必要がある（MUST）。特権操作を実行するためのPIVカード活性化は、カード保有者ま

[3] PIV CHUID の読み出しは特権操作と見なされない。

[4] この文脈における「活性化」（activation）とは、特権操作を実行できるように PIV カードのロックを解除することを意味する。

たは適切なカード管理システムの認証が完了した後にのみ行われるものとする（SHALL）。カード保有者の認証については 4.1.6.1 項で、また、カード管理システムの認証については 4.1.6.2 項で説明する。

4.1.6.1 カード保有者による活性化

PIV カードには、カードに格納された PIV クレデンシャルを使用して特権操作を実行するための、カード保有者による PIN ベースの活性化機能が実装されるものとする（SHALL）。カード保有者による PIN ベースの活性化処理では、数字で構成される PIN をカード保有者が提示しなければならない（SHALL）。この PIN は PIV カードに伝送され、カードによって照合されるものとする（SHALL）。提示された PIN が正しい場合、当該 PIV カードは活性化される。PIV カードは、カードが紛失または盗難にあった場合に悪意の者が試行可能な推測の回数を制限するメカニズムを備えるものとする（SHALL）。また、容易に推測され得る PIN や個人情報から特定され得る PIN（社会保障番号または電話番号の一部など）を使用することは望ましくない（SHOULD NOT）。PIN 認証メカニズムは、FIPS PUB 140-2 Level 2 [FIPS140-2]に規定されたアイデンティティベースの認証要件を満たすものとする（SHALL）。

4.1.6.2 カード管理システムによる活性化

PIV カードは、カードのパーソナライゼーションと発行後のカード更新を行うための、カード管理システムによる活性化機能をサポートしてもよい（MAY）。パーソナライゼーションやカード更新のためにカードを活性化する場合、カード管理システムは[SP800-73]の規定に従い、カードに格納された暗号鍵を使用するチャレンジ／レスポンスプロトコルを実行するものとする（SHALL）。PIV カード管理鍵は、パーソナライズされる際にカード固有の内容に設定されるものとする（SHALL）。つまり、個々の PIV カードにはそれぞれ固有のカード管理用鍵が格納されるものとする（SHALL）。カード管理鍵は、SP 800-78『Cryptographic Algorithms and Key Sizes for Personal Identity Verification』[SP 800-78]に規定されるアルゴリズムおよび鍵サイズ要件を満たすものとする（SHALL）。

4.2 カード保有者ユニーク識別子（CHUID）

CHUID データオブジェクトについては、『PACS Implementation Guidance』[PACS]において定義され、[SP800-73]においてその記述内容が詳細化されている。PIV カードには、[SP800-73]の定義に基づく CHUID が格納されるものとする（SHALL）。CHUID には、個々のカードを一意に識別する連邦機関スマートクレデンシャル番号（FASC-N：Federal Agency Smart Credential Number）という要素が含まれる。CHUID のうち本規格に特有の要素については、下の 4.2.1 項で説明する。CHUID 署名要素の形式については 4.2.2 項で説明する。

PIV の CHUID には、PIV カードを活性化することなく接触型および非接触の両インタフェースを介してアクセスできるものとする（SHALL）。PIV の FASC-N が発行後に変更されてはならない（SHALL NOT）。

4.2.1 PIV CHUIDのデータ要素

PIV カードの識別に使用する必須の FASC-N に加え、CHUID には有効期限の日付データ要素が含まれるものとする（SHALL）。有効期限データ要素は、機械式読み取りが可能な形式で当該カードの有効期限を示すものとする（SHALL）。有効期限の日付形式およびエンコーディング規則については、[SP800-73]の指定に従う。PIV カードの場合、非対称署名フィールドの形式は 4.2.2 項において指定される。

4.2.2 CHUIDの非対称署名フィールド

本規格において、CHUIDコンテナに非対称署名（Asymmetric Signature）フィールドを含めることは必須である。PIV CHUIDの非対称署名データ要素は、RFC 3852 [RFC3852]の定義に従い、Cryptographic Message Syntax（暗号メッセージ構文、以下CMSと称す）の外部ディジタル署名としてエンコーディングされるものとする（SHALL）。このディジタル署名は、非対称署名フィールドを除くCHUID全体の内容に対して算出されるものとする（SHALL）。非対称署名のアルゴリズムおよび鍵サイズ要件については、[SP800-78]で詳細に規定されている。

発行元の非対称署名ファイルは、[RFC3852]の指定に従い *SignedData* タイプとして実装され、次の情報を含むものとする（SHALL）。

+ メッセージ内には、バージョンv3を示す *version* フィールドを含むものとする（SHALL）
+ *digestAlgorithms* フィールドは[SP800-78]の指定に従うものとする（SHALL）
+ *encapContentInfo* の内容は次の規定に従うものとする（SHALL）
  - *eContentType* に id-PIV-CHUIDSecurityObject を指定
  - *eContent* フィールドは省略
+ *certificates* フィールドには、*SignerInfo* フィールドの署名を検証するために使用できる単一の X.509 証明書のみを含むものとする（SHALL）
+ *crls* フィールドは省略（SHALL）
+ *signerInfos* は存在し、単一の *SignerInfo* のみ含むものとする（SHALL）
+ *SignerInfo* の内容は次の規定に従うものとする（SHALL）
  - SignerIdentifier として issuerAndSerialNumber を選択
  - [SP800-78]に従った *digestAlgorithm* を指定
  - 少なくとも次の署名済み属性を含む
    - *MessageDigest* 属性として、非対称署名フィールドを除くCHUIDの連結内容に対して算出されたハッシュ
    - *pivSigner-DN* 属性として、当該CHUIDに署名した主体のPKI証明書に表示される主体者名
  - ディジタル署名を含む

ディジタル署名の検証に必要な公開鍵は、[COMMON]に基づいて発行されたX.509ディジタル署名用証明書の証明書フィールドに含まれているものとする（SHALL）。この公開鍵は4.3項に規定するPIVディジタル署名鍵の形式およびインフラストラクチャ要件を満たすものとする（SHALL）。また、証明書のextendedKeyUsage拡張にはid-PIV-content-signingが設定されなければならない（SHALL）。PIVオブジェクト識別子についての詳細な説明は、付録Dに示す。

4.3 暗号技術仕様

PIV カード上には少なくとも 1 個の非対称プライベート鍵とそれに対応する公開鍵証明書を格納し、その非対称プライベート鍵を使用して暗号演算操作を実行する必要がある（MUST）。この鍵による暗号演算操作は、接触型インタフェースを介してのみ実行できる。

PIV カードには、次の暗号演算操作およびサポート機能を実装するものとする（SHALL）。

+ RSA または楕円曲線暗号による鍵ペア生成
+ RSA または楕円曲線プライベート鍵による暗号演算操作
+ X.509 証明書のインポートおよび格納

追加の非対称鍵および PKI 証明書を PIV カードに格納することもできる（MAY）。本規格では、ディジタル署名および鍵管理鍵に関する要件を定義する。ディジタル署名鍵がサポートされている場合においては、PIV カードに安全なハッシュアルゴリズムを実装する必要はない（NOT REQUIRED）。メッセージのハッシュ処理はカード外で実行してもよい（MAY）。暗号演算操作は非接触インタフェースについては必須でないが、省庁および政府機関の裁量により、カード認証鍵を格納する能力とともに基本的な機能を提供し、対応する各種の暗号演算操作をサポートすることができる（MAY）。たとえば、特定の省庁または政府機関において物理アクセスに次世代標準暗号化方式（AES：Advanced Encryption Standard）ベースのチャレンジ／レスポンスを利用する場合、PIV カードには AES 鍵を格納し、非接触インタフェースを介して AES 操作を実行する機能のサポートが必要となる（MUST）。また、非接触インタフェースで非対称暗号技術（楕円曲線暗号[ECC]など）を利用する場合には、これに対応する公開鍵証明書を格納するための領域を、PIV カードに設ける必要があることもある（MAY）。

PIV 鍵を使用する暗号演算操作は、すべてカード上で実行されるものとする（SHALL）。PIV カード上に追加的な暗号メカニズムを実装することで追加的な暗号機能（ハッシュ生成、署名検証など）をカードに実装する必要はない。各 PIV 鍵タイプごとのアルゴリズムおよび鍵サイズについては、[SP800-78]で指定されている。

PIV カードには次のとおり、必須の鍵が 1 種類と、任意使用の鍵が 4 種類ある。

+ *PIV 認証鍵*は、相互運用可能な環境におけるカード認証をサポートする非対称プライベート鍵であるものとする（SHALL）。これはすべての PIV カードに必須である。
+ *カード認証鍵*は、物理アクセス用の対称（秘密）鍵または非対称プライベート鍵のいずれかであり（MAY）、使用は任意（OPTIONAL）である。
+ *ディジタル署名鍵*は、文書に対する署名をサポートする非対称プライベート鍵であり、使用は任意（OPTIONAL）である。
+ *鍵管理鍵*は、鍵の確立および伝送をサポートする非対称プライベート鍵であり、使用は任意（OPTIONAL）である。この鍵は暗号化鍵としても使用できる。
+ *カード管理鍵*は、パーソナライゼーションおよび発行後の管理活動に使用される対称鍵であり、使用は任意（OPTIONAL）である。

すべての PIV 暗号鍵は、全体として FIPS 140-2 により Level 2 以上の認定された暗号モジュールにより生成されるものとする（SHALL）。全体として Level 2 の認定に加え、PIV カードは格納された PIV プライベート鍵を保護するための Level 3 物理セキュリティを備えるものとする（SHALL）。

鍵の種別に応じた格納およびアクセスに関する固有の要件についての詳細を次に示す。該当する項目については鍵管理上の要件もあわせて示す。

+ **PIV 認証鍵**:この鍵は PIV カード上で生成されるものとする(SHALL)。PIV カードは PIV 認証鍵のエクスポートを許可してはならない(SHALL NOT)。PIV 認証鍵の使用は、PIV カードの接触型インタフェースを介してのみ可能としなければならない(MUST)。プライベート鍵操作は、活性化された PIV カードを使用することにより、ユーザの明示的な操作を伴わずに実行できる(MAY)(たとえば、個々の操作ごとにユーザが PIN を提示する必要はない)。

  PIV カードには、対応する X.509 証明書が公開鍵の有効性確認サポート用に 1 個格納されるものとする(SHALL)。この X.509 証明書の subject alternative name 拡張には、pivFASC-N 属性を使用し、物理アクセス手順をサポートするための FASC-N が含まれるものとする(SHALL)。証明書の有効期限は、当該 PIV カードの有効期限よりも後の日付であってはならない(MUST)。PIV 認証用証明書には PIV NACI indicator 拡張を含むこと(SHALL)。この重要度が高くないプライベート拡張は、カード発行時点における対象の身元調査の状況を示す。本文書の 5.4 項では、PIV 認証鍵のための証明書形式および鍵管理インフラストラクチャについて指定する。

+ **カード認証鍵**:PIV カードはカード認証鍵のエクスポートを許可してはならない(SHALL NOT)。プライベート鍵/秘密鍵の操作は、この鍵を使用することにより、ユーザの明示的な操作を伴わずに実行できる(MAY)(たとえば、ユーザが PIN を提示する必要はない)。本規格では、鍵管理プロトコルまたはインフラストラクチャ要件については指定しない。

+ **ディジタル署名鍵**:PIV ディジタル署名鍵は PIV カード上で生成されるものとする(SHALL)。PIV カードはディジタル署名鍵のエクスポートを許可してはならない(SHALL NOT)。存在する場合、ディジタル署名鍵を使用する暗号演算操作は PIV カードの接触型インタフェースを介してのみ実行できる(MAY)。プライベート鍵操作は、ユーザの明示的な操作を伴わずには実行できない(MAY NOT)。

  PIV カードには、対応する X.509 証明書がディジタル署名鍵の有効性確認サポート用に 1 個格納されるものとする(SHALL)。本文書の 5.4 項では、PIV ディジタル署名鍵のための証明書形式および鍵管理インフラストラクチャについて指定する。

+ **鍵管理鍵**:この鍵は PIV カード上で生成されるか、カードへとインポートされる(MAY)。存在する場合、鍵管理鍵へのアクセスは、PIV カードの接触型インタフェースを介してのみ可能としなければならない(MUST)。プライベート鍵操作は、発効された PIV カードを使用することにより、ユーザの明示的な操作を伴わずに実行できる(MAY)(たとえば、個々の操作ごとにユーザが PIN を提示する必要はない)。この鍵は暗号化鍵とも呼ばれることがある。

  PIV カードには、対応する X.509 証明書が鍵管理鍵の有効性確認サポート用に 1 個インポートおよび格納されるものとする(SHALL)。本文書の 5.4 項では、PIV 鍵管理鍵のための証明書形式および鍵管理インフラストラクチャについて指定する。

+ **カード管理鍵**:カード管理鍵は、発行元によってカードへとインポートされる。存在する場合、カード管理鍵へのアクセスは、PIV カードの接触型インタフェースを介してのみ可能としなければならない(MUST)。詳細については 4.1.6.2 項を参照のこと。

PIV カードには、PKI パス有効性確認用の X.509 証明書もインポートおよび格納できる(MAY)。それらトラストアンカー証明書には、カード保有者の明示的な操作を伴わずに活性化された PIV カー

ドを使用することにより接触型インタフェースを介してアクセスできる（MAY）。サポートされる場合、トラストアンカー証明書の初期化および更新には、カードの活性化だけでなくカード保有者の明示的な操作も要求されるものとする（SHALL）。

4.4 バイオメトリックデータ仕様

PIV カードのライフサイクル中に使用されるバイオメトリックデータは、次の要素により構成されるものとする（SHALL）。

+ アイデンティティの立証および登録プロセスの一環として法執行機関によるチェックを実行するために使用される、指紋の完全なセット
+ カード上への顔写真印刷、およびカード使用期間中の視覚的認証を実行するために使用される顔写真画像。再発行時には必ず新しい顔写真画像を採取する必要がある（MUST）。顔写真画像はカード上に格納される必要はない（NOT REQUIRED）
+ カード利用時にの自動認証に使用される、2 つの指紋

上記 3 つのバイオメトリックデータは、アイデンティティの立証および登録プロセスの一環として採取される。PIV カード上へのバイオメトリックデータ格納に関する実装要件は、NIST SP 800-76 [SP800-76]に規定される仕様の採用方法に応じて異なる。

カード上に格納される 2 つの指紋には、接触型インタフェースを介してのみ、かつ、有効な PIN の提示後にのみアクセスできるものとする（SHALL）。本規格では、PIV カード上に格納することを指定しているバイオメトリックデータに対する非接触インタフェース経由でのアクセスを認めない。

4.4.1 バイオメトリックデータの採取、格納、および使用

指紋の完全なセットは、これを提供可能なすべての PIV カード申請者から採取するものとする（SHALL）。10 個の指紋の採取および形式に関する技術仕様は、[SP800-76]に規定されている。これらの指紋は、FBI の維持管理する指紋データベースに対する 1 対多照合に使用されるものとする（SHALL）。指紋の読み取りには FBI 認定のスキャナを使用し、伝送には FBI 標準のトランザクションを使用することが望ましい（SHOULD）。この 1 対多照合処理はバイオメトリック識別と呼ばれる。10 個の指紋に関する要件は、NIST による大規模試験で得られた照合正確性データに基づいており、NISTIR 7123 [NISTIR7123]において報告されている。指紋を使用したバイオメトリック識別は法執行機関によるチェックの主要な手段であるため、政府機関は、10 個の指紋を取得することが不可能な場合の法執行機関によるチェックの代替手段について人事局（OPM）のガイダンスを求めること（SHALL）。

顔写真画像はすべての PIV 申請者から採取するものとする（SHALL）。顔写真画像に関する技術仕様については、[SP800-76]に規定されている。顔写真画像は次の用途に使用できる（MAY）。

+ カード表面に印刷される画像の生成
+ 6.2.1 項に定義された視覚認証プロセスを補強するために守衛ワークステーションのモニタに表示する画像の生成。このアプローチは次の状況で必要になる場合がある（MAY）
  - 指の負傷または欠損により、PIV カード保有者から現在の良好な指紋サンプルを採取できない場合
  - 指紋照合設備の故障

- リハビリテーション法第 508 条の適用対象となっている PIV カード保有者を認証する場合

2 つの指紋は、これを提供可能なすべての PIV カード申請者から、カードへの格納用に採取するものとする（SHALL）。または、先に法執行機関チェック用として採取した 10 個の指紋から 2 個を抽出してこれらの指紋としてもよい。2 つの指紋に関する技術仕様については、[SP800-76]に規定されている。通常は、右手の人差し指と左手の人差し指をそれぞれ第 1 および第 2 の指として使用するものとする（SHALL）。ただし、これらの指を画像にできない場合には、次の順序で使用可能な指を上から順に第 1、第 2 の指として使用するものとする（SHALL）。

1. 右手の親指
2. 左手の親指
3. 右手の中指
4. 左手の中指
5. 右手の薬指
6. 左手の薬指
7. 右手の小指
8. 左手の小指

これらの指紋は、PIV カード保有者から採取した現在のサンプルに対して 1 対 1 バイオメトリック検証のため照合されるものとする（SHALL）（6.2.3 項を参照）。カード上には 2 つの指紋が格納されているが、PIV カード保有者の認証を目的としていずれか一方の指紋または両方の指紋を使用するかについては、省庁または政府機関の裁量による。ひとつの指紋のみ認証に使用する場合、第 1 の指を優先して使用すること（SHALL）。許容可能な品質の指紋をひとつたりとも採取することが困難である場合は、該当省庁または政府機関において、6.2.4 項に規定する非対称暗号を使用した認証を実行するものとする（SHALL）。

4.4.2 バイオメトリックデータの表現および保護

バイオメトリックレコードの形式は、バイオメトリックのタイプ（指紋、顔、手の寸法など）によって異なる。1 つ以上のレコードを連結して汎用レコードヘッダの後に付加することにより、標準バイオメトリックレコード（STD_BIOMETRIC_RECORD と呼ばれる）が形成される。標準バイオメトリックレコードの前には共通バイオメトリック交換形式フレームワーク（CBEFF：Common Biometric Exchange Formats Framework）ヘッダ（CBEFF_HEADER と呼ばれる）が付加され、また、後には CBEFF 署名ブロック（CBEFF_SIGNATURE_BLOCK と呼ばれる）が付加される。[CBEFF] CBEFF_SIGNATURE_BLOCK は当該バイオメトリックデータのディジタル署名を含み、したがってバイオメトリックデータの完全性の検証に役立つ。PIV カード上のバイオメトリックデータ表現をも含む完全な CBEFF の構造は次の要素により構成される。

+ CBEFF_HEADER
+ STD_BIOMETRIC_RECORD
+ CBEFF_SIGNATURE_BLOCK

CBEFF_HEADER および STD_BIOMETRIC_RECORD の形式は、[SP800-76]に指定されている。CBEFF_SIGNATURE_BLOCK の生成プロセスは次に説明するとおりである。CBEFF_SIGNATURE_BLOCK は、[RFC3852]に定義される CMS 外部ディジタル署名としてエンコ

ーディングされるものとする（SHALL）。このディジタル署名は、CBEFF_SIGNATURE_BLOCK 自体を除く CBEFF 構造全体の内容に対して算出されるものとする（SHALL）（つまり、CBEFF_HEADER および STD_BIOMETRIC_RECORD は含まれる）。ディジタル署名のアルゴリズムおよび鍵サイズ要件は、[SP 800-78]で詳細に規定されているとおりである。

CBEFF_SIGNATURE_BLOCK の CMS エンコーディングは *SignedData* タイプであり、次の情報を含むものとする（SHALL）。

+ メッセージ内には、バージョン v3 を示す *version* フィールドを含むものとする（SHALL）
+ *digestAlgorithms* フィールドは[SP800-78]の指定に従うものとする（SHALL）
+ *encapContentInfo* の内容は次の規定に従うものとする（SHALL）
  - *eContentType* に id-PIV-biometricObject を指定
  - *eContent* フィールドは省略
+ バイオメトリックの署名を生成した際の鍵が CHUID の署名を生成した鍵と同じである場合、*certificates* フィールドは省略されるものとする（SHALL）
+ バイオメトリックの署名を生成した際の鍵が CHUID の署名を生成した鍵と異なる場合、*certificates* フィールドには、*SignerInfo* フィールドの署名の検証に使用できる単一の証明書のみを含むものとする（SHALL）
+ *crls* フィールドは省略（SHALL）
+ *signerInfos* は存在し、単一の *SignerInfo* のみ含むものとする（SHALL）
+ *SignerInfo* の内容は次の規定に従うものとする（SHALL）
  - SignerIdentifier として issuerAndSerialNumber を選択
  - [SP800-78]に従った *digestAlgorithm* を指定
  - 少なくとも次の署名済み属性を含む
    - *MessageDigest* 属性として、連結された CBEFF_HEADER + STD_BIOMETRIC_RECORD に対するハッシュ
    - *pivFASC-N* 属性として、PIV カードの FASC-N（バイオメトリックデータと PIV カードとをリンクするため）
    - *pivSigner-DN* 属性として、当該バイオメトリックデータに署名した主体の PKI 証明書に表示される主体者名
  - ディジタル署名を含む

ディジタル署名の検証に必要な公開鍵を含んだ X.509 ディジタル署名用証明書は、[COMMON]に基づいて発行されたものとする（SHALL）。この証明書は 4.3 項に規定する PIV ディジタル署名鍵の形式およびインフラストラクチャ要件を満たすものとする（SHALL）。また、証明書の extendedKeyUsage 拡張には id-PIV-content-signing が設定されなければならない（SHALL）。PIV オブジェクト識別子についての詳細な説明は、付録 D に示す。

本規格では、PIV バイオメトリックデータの平文による読み出しが不可能であること、および PIN などの認証メカニズムによって保護されることを必須とする。ただし、その他のバイオメトリック情報を接触型または非接触 IC 内に格納すべきかどうかについては指定しない。非接触 IC に格納されたバイオメトリック情報に対する無許可のアクセスを防ぐため、電磁シールドケースなどの技術による保護は必須である（REQUIRED）。

4.4.3 バイオメトリックデータの内容

照合正確性およびデータ相互運用性は、PIV カードのバイオメトリックデータ形式を指定する際の主要な要素である。これらのデータ特性には、画像レコード内の画像パラメータ（ピクセル密度、ピクセル深度など）や、それを格納する標準のバイオメトリックレコードが持つフィールドが含まれる。すでに述べたとおり、PIV のライフサイクルにおいて収集されるバイオメトリックデータの内容については[SP800-76]において概要が説明されている仕様に従うものとする（SHALL）。

4.5 カードリーダの仕様

本項では、接触型および非接触カードリーダに関する最低限の要件を示す。また、PIN 入力デバイスの最低限の要件についても示す。

4.5.1 接触型リーダの仕様

接触型カードリーダのカード／リーダ間インタフェースについては、[ISO7816]規格に準拠するものとする（SHALL）。汎用デスクトップコンピュータ環境におけるリーダ／ホスト間インタフェースについては、『Personal Computer/Smart Card (PC/SC) Specification（パーソナルコンピュータ／スマートカード間仕様）』[PCSC]に準拠するものとする（SHALL）。物理アクセス制御システムにおいて、リーダが汎用デスクトップコンピュータ環境に接続されていない場合のリーダ／ホスト間インタフェースについては、本規格では指定しない。

4.5.2 非接触リーダの仕様

非接触カードリーダのカード／リーダ間インタフェースについては、[ISO 14443]規格に準拠するものとする（SHALL）。リーダが汎用デスクトップコンピュータ環境に接続されている場合のリーダ／ホスト間インタフェースについては、[PCSC]に準拠するものとする（SHALL）。物理アクセス制御システムにおいて、リーダが汎用デスクトップコンピュータ環境に接続されていない場合のリーダ／ホスト間インタフェースについては、本規格では指定しない。そのような形態は、さまざまな非標準のカードリーダ通信インタフェースを使用する既存の物理アクセス制御システムに後から PIV リーダを取り付ける場合に必要とされる。

4.5.3 PIN入力デバイスの仕様

PIN 入力デバイスは、PIN ベースの PIV カード活性化機能を実装する場合に使用するものとする（SHALL）。PIV カードを PIN と併用して物理アクセスを行う場合は、リーダと統合された PIN 入力デバイスを使用するものとする（SHALL）。PIV カードを PIN と併用して論理アクセス（Web サイトまたはその他サーバに対する認証など）を行う場合、リーダと統合された PIN 入力デバイスを使用するか、コンピュータのキーボードを使用して PIN を入力する（MAY）。PIN 入力デバイスがリーダと統合されていない場合、PIN はカード活性化のために安全かつ直接的な方法で PIV カードに伝送されるものとする（SHALL）。

5. PIVカードの発行および管理サブシステム

本セクションでは、PIV-II 実装においてカード発行および管理サブシステムの構成要素となるプロセスのセキュリティ要件を定義する。PIV-I の要件と合致する部分も多いが、相互運用可能な PIV カードの発行および管理に関する要件を含むほか、PIV カードでサポートされる論理クレデンシャルの発行および管理に関する追加的なセキュリティ要件についても規定する。PIV-II システムの実装に関する技術仕様は、本規格のセクション 4 と、NIST SP 800-73 および NIST SP 800-76 において説明している。

5.1 管理目標および相互運用要件

[HSPD-12]は、連邦職員および業務請負企業を安全かつ高い信頼性で識別するための管理目標を定めた。大統領指令の第 3 項に記載されている、これらの管理目標を以下に示す:

> (3)この指令における「安全かつ高い信頼性のアイデンティティ」とは、(a)個々の職員のアイデンティティを検証するための確かな基準に基づいて発行され、(b)身元詐称、アイデンティティの改ざん、偽造、テロリストによる利用に対する強い耐性を有し、(c)電子的な認証が迅速に行え、(d)公式の認定プロセスによって信頼性が確立されているプロバイダのみが発行するアイデンティティを意味する。

PIV-I が規定する要件は、PIV-II においても保持される。各政府機関の PIV 実装は、上記(a)から(d)の管理目標を満たさなければならない(SHALL)。

また、大統領令[HSPD-12]には、政府全体におけるアイデンティティクレデンシャルの相互運用性に関する要件が規定されている。それらの要件は、この大統領令の第 1 項に次に引用するとおり記載されており、PIV-II においては必須である(REQUIRED)。

> (1)テロリストの攻撃を受ける可能性がある連邦政府施設およびその他の施設に対してのアクセスに使用される各種形態の身元証明については、品質およびセキュリティの広範な多様性を排除する必要がある。したがって、連邦政府から職員および委託業者(委託業者の従業員を含む)に対して発行される身元証明に関して、強制力を有し政府全体を対象とした安全かつ高い信頼性を有する形態の標準を確立することにより、政府全体としてのセキュリティを強化し、政体を効率化し、身元詐称の発生を抑制し、個人のプライバシを保護することが、合衆国としてのポリシーである。

各政府機関の PIV 実装においては、セクション 4 に指定される相互運用可能な PIV カードおよびそれに関連する論理クレデンシャルを発行および管理することにより、相互運用性をサポートしなければならない(SHALL)。

5.2 PIVアイデンティティの立証と登録の要件

本規格の 2.2 項では、アイデンティティの立証および登録に関して承認されたプロセスを採用および運用することを義務付けている。PIV-II におけるアイデンティティの立証および登録システムはすべて、この承認を受けるために、2.2 項に示す PIV-I の目標および要件を満たさなければならない(MUST)。NACI または同等の調査が完了していない個人に対して発行されたアイデンティティクレデンシャルと、調査が完了した個人に対して発行されたアイデンティティクレデンシャルとは、電子的に区別可能である必要がある(MUST)。

PIV-II における追加要件の 1 つとして、PIV カードをパーソナライズするために使用されるバイオメトリック(指紋および顔写真画像)はアイデンティティの立証および登録プロセスの間に採取する必要がある(MUST)。

PIV カードの発行時、連邦政府省庁および政府機関はアイデンティティの立証および登録に関して承認されたプロセスを採用する必要がある（MUST）。PIV アイデンティティの立証および登録に関して承認された 2 つのプロセスを付録 A に示す。その他のアイデンティティ立証および登録プロセスは、必須とされる PIV の目標および要件を満たすことを該当省庁または政府機関によって認定され、該当する連邦政府省庁または政府機関の長の書面による承認を得た場合に使用できる（MAY）。

5.3 PIVの発行と維持管理の要件

5.3.1 PIVカードの発行

本規格の 2.2 項では、発行および維持管理に関して承認されたプロセスを採用および運用することを義務付けている。PIV-II における発行および維持管理システムはすべて、この承認を受けるために、2.3 項に示す PIV-I の目標および要件を満たさなければならない（MUST）。職員または委託業者は、連邦職員の採用時に要求される NACI あるいは OPM または国家安全保障コミュニティによる他の調査が継続中である間、PIV カードおよび論理クレデンシャルの発行を受けることができる(2.2 項を参照)（MAY）。これに該当する場合は、調査の完了および審査の通過が当該プロセスにおいて確認される必要がある（MUST）。

追加要件の 1 つとして、発行元は、PIV カードまたは PIV 登記レコードに含まれるバイオメトリックに対して申請者の 1 対 1 バイオメトリック照合を行わなければならない（SHALL）。合致が確認された場合に、PIV カードが申請者に対して発行されるものとする（SHALL）。

必須とされる PIV-II の目標および要件を満たす PIV 発行プロセスの 2 つの例を、付録 A の A.1.2 項、および付録 A の A.2.2 項から A.2.4 項に示す。連邦政府省庁および政府機関の長は、必須とされる PIV-I の目標および要件を満たすことが承認されたアイデンティティの立証、登録および発行プロセスに関して、使用を承認できる（MAY）。発行プロセスは、各省庁および政府機関に特有の制約および要件に応じて拡張することもできる（MAY）。

5.3.2 PIVカードの維持管理

PIV カードの維持管理は、本項の指定に適合する方法で行うものとする（SHALL）。

PIV カードの有効期間が終了するのに先立ち、カードに記録されているデータおよびクレデンシャルを無効化する必要が生じる場合がある（MAY）。カード保有者は退職または転職する場合や解雇される場合があり（MAY）、それまで有効であったカードを失効させる必要が生じることがある。また、カードは破損、紛失もしくは盗難にあう場合があり（MAY）、代替のカードが必要となることがある。PIV システムでは、この情報が PIV 管理インフラストラクチャ内に効率的に伝播し、カード保有者の認証を行う組織に提供されることを保証しなければならない（MUST）。この意味において、PIV カード維持管理の手順は、効率的なカード管理が保証されるよう省庁および政府機関における処理手順に統合されている必要がある（MUST）。

5.3.2.1 PIVカードの更新

更新とは、完全な登録手続きを繰り返すことなく PIV カードを発行し直すプロセスである。カード発行者は、カードおよびそれに関連付けられたクレデンシャルの更新に先立ち、当該職員の身元が確実であること、および人事記録の内容が最新であることを確認しなければならない（SHALL）。現行の職員に対するアイデンティティクレデンシャルを更新する際には OPM のガイダンスに従って NACI 調査を実施すること（SHALL）。

PIV カードの有効期間は 5 年間を超えないものとする（SHALL）。カード保有者は、有効な PIV カードの有効期間が終了する 6 週間前から実際の有効期限までの間に更新を申請することが認められるものとする（SHALL）。カード発行者は、期限切れ前のカードに格納されているバイオメトリック情報と照合することによりカード保有者の本人性を検証する。期限切れの PIV カードは回収・破壊されなければならない（MUST）。

更新前のバイオメトリックデータは更新後の PIV カードに再使用してよい（MAY）が、ディジタル署名は更新後の FASC-N によって算出し直す必要がある（MUST）。

PIV 認証用証明書および任意使用のディジタル署名用証明書の有効期限は、当該 PIV カードの有効期限よりも後の日付であってはならない。この要件に従って新しい PIV 認証鍵および証明書を生成すること（SHALL）。任意使用の鍵管理鍵をサポートする PIV カードの場合、鍵認証鍵は新しい PIV カードにインポートしてもよい（MAY）。

5.3.2.2 PIVカードの再発行

再発行の際には、指紋および顔写真画像の採取を含め、登録および発行プロセスの全体を実行するものとする（SHALL）。カード発行者は、カードおよびそれに関連付けられたクレデンシャルの再発行に先立ち、当該職員の身元が確実であること、および人事記録の内容が最新であることを確認しなければならない（SHALL）。

カード保有者は、PIV カードの不正使用、紛失、盗難、または破損が生じた場合、新しい PIV カードの再発行を申請しなければならない（SHALL）。また、カード保有者の雇用の形態や属性に変更が生じた場合、もしくは 1 つ以上の論理クレデンシャルの信頼性が失われた場合にも、カード保有者は再発行を申請できる。

上記いずれかの事態が報告された場合、通常の運用手順により次の事項が確実に実施される必要がある（MUST）。

+ PIV カード自体を失効させること。現在有効（または無効）な FASC-N 値を示すローカルデータベースすべてを更新し、状態の変化を反映すること（MUST）。
+ CA（認証局）に通知し（SHALL）、当該 PIV カード上の PIV 認証鍵に対応する証明書を失効させること（MUST）。任意使用の（OPTIONAL）ディジタル署名および鍵管理鍵が使用されている場合は、省庁および政府機関がこれらに対応する証明書を失効させること。発行される証明書失効リスト（CRL）に、該当する証明書のシリアル番号を含めること（SHALL）。
+ オンライン証明書状態プロトコル（OCSP：Online Certificate Status Protocol）レスポンダを更新し、当該 PIV カード上の証明書に関する照会に対し適切な応答を返すようにすること（SHALL）。これは、間接的な方法（上記の CRL の公開による）と、直接的な方法（OCSP サーバ内部の失効レコードを更新することによる）とのいずれかで行うことができる（MAY）。

以前の PIV カードを入手できる場合は、これを回収し破壊することを推奨する（RECOMMENDED）。カードの回収が不可能な場合は、通知の時点から 18 時間以内に通常の運用手順を完了すること（SHALL）。ただし、場合によっては 18 時間の遅延が許容されないことがある。その場合は緊急時手順を実行し、可能な限り速やかに当該情報を伝播させなければならない（MUST）。省庁および政府機関には、そのような場合に緊急時告知を発行する手順を整備しておくことが要求される（REQUIRED）。

5.3.2.3 PIVカードおよびPINのリセット

該当省庁または政府機関の規定する許容試行回数を超えて無効な PIN が使用された結果、PIV カードの内容がロックされた場合は、カード上の PIN のリセットが必要になることがある（MAY）。PIN のリセットはカード発行者が実行できる（MAY）。リセット後の PIV カードをカード保有者に返却する前に、カード発行者は、保有者のバイオメトリックとリセット後の PIV カードに格納されたバイオメトリックが合致することを確認すること（SHALL）。省庁および政府機関は必要に応じて、より厳格な PIN リセット手順（PIN リセットの禁止、ロックされた PIV カードの利用停止を含む）を採用することができる（MAY）。その場合、当該手順は省庁および政府機関によって公式に文書化されなければならない（SHALL）。

5.3.2.4 PIVカードの利用停止

利用停止プロセスは、カードとそれに格納されたデータおよび鍵を永久に破壊または無効化し、それ以降の再使用を不可能にするために実行される。PIV カードの利用停止は次の状況において実行されるものとする（SHALL）。

+ 職員が（自発的または非自発的に）連邦政府の職務から離脱する場合
+ 職員が（自発的または非自発的に）連邦政府の委託業者から離脱する場合
+ 委託業者が、作業場所の変更により連邦政府の建造物またはシステムにアクセスする必要がなくなる場合
+ カード保有者が、虚偽のアイデンティティを所持していると判明した場合
+ カード保有者が死亡した場合

カードまたはクレデンシャルの不正使用が発生した場合と同様、通常の利用停止手順により次の事項が確実に行われる必要がある（MUST）。

+ PIV カードを回収・破壊すること。
+ PIV カード自体を失効させること。現在有効（または無効）な FASC-N 値を示すローカルデータベースすべてを更新し、状態の変化を反映すること（MUST）。
+ CA（認証局）に通知し（SHALL）、当該 PIV カード上の PIV 認証鍵に対応する証明書を失効させること（MUST）。任意使用の（OPTIONAL）ディジタル署名および鍵管理鍵が使用されている場合は、省庁および政府機関がこれらに対応する証明書を失効させること。発行される CRL に、該当する証明書のシリアル番号を含めること（SHALL）。
+ OCSP レスポンダを更新し、当該 PIV カード上の証明書に関する照会に対し適切な応答を返すようにすること（SHALL）。これは、間接的な方法（上記の CRL の公開による）と、直接的な方法（OCSP サーバ内部の失効レコードを更新することによる）とのいずれかで行うことができる（MAY）。
+ カード保有者から採取した IIF を、当該省庁または政府機関における所定のプライバシポリシーおよびデータ保持ポリシーに従って破棄すること。

5.4 PIV鍵管理の要件

本仕様に合致するPIVカードには、1つ以上の非対称プライベート鍵が格納される。これらの非対称プライベート鍵に関連付けられた公開鍵を管理するために、省庁および政府機関は次に定めるX.509公開鍵証明書を発行および管理する必要がある（REQUIRED）。

5.4.1 アーキテクチャ

PIVカード認証をサポートする証明書の発行元であるCAは、連邦政府PKIにより管理される共通ポリシー（Common Policy）用のPKI階層構造に所属していなければならない（SHALL）。これらのCAにより発行される自己署名用証明書、自己発行証明書、CA証明書は、それぞれ『X.509 Certificate and CRL Profile for the Common Policy（共通ポリシーのための X.509 証明書およびCRL プロファイル）』[PROF]のワークシート1「*Self-Signed Certificate Profile*（自己署名用証明書プロファイル）」、ワークシート2「*Self-Issued CA Certificate Profile*（自己発行 CA 証明書プロファイル）」およびワークシート3「*Cross Certificate Profile*（横断認証証明書プロファイル）」に適合しなければならない（SHALL）。レガシーPKIに関する要件は5.4.4項で定義される。

5.4.2 PKI証明書

PIVカード認証をサポートする目的で発行されるすべての証明書は、『*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*（合衆国連邦政府PKI共通ポリシーフレームワークのためのX.509 証明書）』[COMMON]で定義されるid-CommonHWポリシーおよびid-CommonAuthポリシー[5]に基づいて発行されなければならない（SHALL）。レガシーPKIに関する要件は5.4.4項で定義される。アイデンティティの立証とCAおよび登録機関の管理は、それらの要件により規定される。CAおよび登録機関は、省庁および政府機関により運営される機関であっても、PKIサービスプロバイダへの外部委託であってもよい（MAY）。[COMMON]に基づく運営が承認されたPKIサービスプロバイダの一覧については、http://www.cio.gov/ficc/cpl.htmを参照のこと。

[COMMON]では、加入者の暗号モジュール（すなわちPIVカード）に対してFIPS 140-2 Level 2の認定を要求している。また、本規格ではカード保有者に対して、PIVカードによりディジタル署名鍵を用いたプライベート鍵による演算を実行するたびにPIVカードを認証することを要求する。

[COMMON]では、RSAを使用することが鍵サイズおよびハッシュ関数とともに指定されている。

本規格ではそれに加え、[SP 800-78]に規定された暗号アルゴリズムおよび鍵サイズの使用を認める。[COMMON]の規定も、将来的には追加のアルゴリズムを認めるよう拡張される見込みである。本規格に適合するために、PIVカード管理システムでは、本規格および現行バージョンの[COMMON]で認められたアルゴリズムおよび鍵サイズのみ使用するものとする。

5.4.2.1 X.509 証明書の内容

PIVプライベート鍵に関連付けられるX.509証明書に求められる内容は[PROF]に基づく。その関係は次に示すとおりである。

+ Authority Information Access（AIA）拡張は、適切なOCSP状態レスポンダへのポインタを含むものとする（SHALL）。このポインタでは、[PROF]で要求されるLDAP(Lightweight Directory Access Protocol: ライトウェイト・ディレクトリアクセスプロトコル、以下LDAPと称

[5] id-CommonAuthポリシーの内容はまだ起案されていない。このポリシーは、ユーザの対話操作を必要としない単純な認証鍵と、操作にユーザの明示的な意思表示を伴うことが前提となる署名鍵とを区別するために使用される予定である。

す) URI（Uniform Resource Identifier）に加え、[PROF]のセクション 8 で指定される id-ad-ocsp アクセスメソッドを使用する。

+ PIV 認証鍵を使用したプライベート鍵による演算処理を、（暗号モジュールの活性化に必須の介入のほかに）ユーザの介入なしに実行できる場合、これに対応する証明書では、certificate policies 拡張に id-CommonHW ではなく id-CommonAuth を指定する必要がある（MUST）。

+ 非対称のカード認証鍵に関連付けられた公開鍵を含んだ証明書では、certificate policies 拡張に id-CommonHW ではなく id-CommonAuth を指定し（MUST）、PIV NACI indicator 拡張を含み（付録 D を参照）（MUST）、かつ、extended key usage 拡張に id-PIV-cardAuth を設定する必要がある（MUST）。

+ ディジタル署名プライベート鍵に関連付けられた公開鍵を含んだ証明書は、[PROF]のワークシート 5「*End Entity Signature Certificate Profile*（エンドエンティティ署名用証明書プロファイル）」に適合しなければならない（SHALL）。

+ PIV 認証プライベート鍵に関連付けられた公開鍵を含んだ証明書は、[PROF]のワークシート 5「*End Entity Signature Certificate Profile*（エンドエンティティ署名用証明書プロファイル）」に適合するものとする（SHALL）が、*keyUsage* 拡張に nonRepudiation ビットを設定すべきでなく（SHALL NOT）、PIV NACI indicator 拡張を含む必要があり（付録 D を参照）（MUST）、かつ、subject alternative name フィールドに当該 PIV カードの FASC-N を含む必要がある（MUST）。

+ 鍵管理プライベート鍵に関連付けられた公開鍵を含んだ証明書は、[PROF]のワークシート 6「*Key Management Certificate Profile*（鍵管理用証明書プロファイル）」に適合しなければならない（SHALL）。

+ 各PIV非対称鍵タイプごとのアルゴリズムおよび鍵サイズ要件については、[SP800-78]で規定されている。[6]

5.4.3 X.509 CRLの内容

PIV プライベート鍵に対応する証明書の発行元である CA は、18 時間ごとに 1 回以上の頻度で CRL を発行しなければならない（SHALL）。X.509 CRL の内容については、[PROF]のワークシート 4「*CRL Profile*（CRL プロファイル）」に適合しなければならない（SHALL）。

5.4.4 レガシーPKIからの移行

連邦ブリッジ認証局（FBCA：Federal Bridge CA）により Medium-HW または High の保証レベルで横断認証（cross-certified）された PKI を使用する省庁および政府機関は、当該省庁および政府機関に特有のポリシーオブジェクト識別子（OID：Object Identifier）を引き続き設定してよい（MAY）。2008 年 1 月 1 日またはそれ以降に発行される証明書には、ポリシーOID として id-CommonHW または id-CommonAuth を設定するものとする（SHALL）（省庁および政府機関では、2008 年 1 月 1 日以降に発行される id-CommonHW および id-CommonAuth のポリシーOID に加え、当該省庁および政府機関に特有のポリシーOID を引き続き設定してよい（MAY））。

[6] 現行の[COMMON]のテキストでは、RSA の SHA-1 および SHA-256 のみ認めている。楕円曲線アルゴリズムのサポートにより[COMMON]の改定が必要になると考えられる。

5.4.5 PKIリポジトリおよびOCSPレスポンダ

PIV PKIリポジトリおよびオンライン証明書状態プロトコル（OCSP：Online Certificate Status Protocol）レスポンダは、機関間で高い信頼性の PIV カード相互運用をサポートするために、省庁、政府機関およびその他の組織について横断的に PIV カードおよび鍵状態情報を提供する。カードまたは証明書を失効させる必要が生じた場合、これを認証局（CA：Certificate Authority）に通知することは省庁および政府機関の責任である。CA は、PIV カードおよび証明書の状態チェックに必要となるサーバおよびレスポンダの状態を維持管理しなければならない（SHALL）。

認証用証明書の有効期限は、当該 PIV カードの有効期限よりも後の日付であってはならない（SHALL NOT）。カードが失効する際には、その認証用証明書も失効しなければならない（SHALL）。ただし、認証用証明書（およびそれに関連付けられた鍵ペア）は、PIV カードの失効を伴うことなく失効する場合や、その後置き換えられる場合がある（MAY）。正当で、有効期限が切れておらず、失効もしていない PIV 認証用証明書がカード上に存在することは、そのカードが発行済みであり失効していないことを証明するものである。

認証用証明書の有効期間は数年にわたり継続するのが普通であるため、証明書の失効処理メカニズムが必要となる。以前から使用されてきたメカニズムとして、CRL および OCSP の 2 種類がある。PIV 認証用証明書の発行元である CA は、自身の発行した証明書、および連邦ブリッジ認証局への経路を構築するために必要なすべての CA 証明書について、CRL を保持する LDAP ディレクトリサーバを維持管理しなければならない（SHALL）。

証明書は、CRL および信ずべき OCSP レスポンダを特定するために必要とされる、*crlDistributionPoints* 拡張または *authorityInfoAccess* 拡張を含まなければならない（SHALL）。また、PIV 認証用証明書の発行元である各 CA は、当該 CA の発行した個々の認証用証明書すべてについての証明書状態を提供する OCSP サーバを運用しなければならない（SHALL）。

5.4.5.1 証明書およびCRLの配布

本規格では、CA 証明書および CRL の配布に LDAP およびハイパーテキスト転送プロトコル（HTTP：Hypertext Transport Protocol）を使用することを要求する。具体的な要件については、『Shared Service Provider Repository Service Requirements（共有サービスプロバイダのリポジトリサービス要件）』[SSP REP]の表 II「Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements（必須リポジトリサービスの LDAP アクセス要件）」に示されている。

PIV 認証用証明書の subject alternative name 拡張には FASC-N が含まれるため、これらの証明書を LDAP または HTTP 経由で一般に配布してはならない（SHALL NOT）。その他のユーザ証明書（ディジタル署名および鍵管理）を LDAP で配布可能かどうかは、個別の省庁および政府機関の裁量により決定してよい。ユーザ証明書を配布する際には、[SSP REP]の表 I「End-Entity Certificate Repository Service Requirements（エンドエンティティ証明書のリポジトリサービス要件）」を満たさなければならない（SHALL）。

5.4.5.2 OCSP状態レスポンダ

補助的な証明書状態メカニズムとして、OCSP [RFC2560]状態レスポンダを実装しなければならない（SHALL）。OCSP 状態レスポンダは、少なくとも CRL の発行と同じ頻度で更新される必要がある（MUST）。各証明書にとっての決定的な OCSP レスポンダは、[PROF]の記述に従って AIA 拡張により指定されるものとする（SHALL）。

5.5 PIVのプライバシ要件

2.4 項で述べた PIV プライバシ要件は、PIV-II 実装にも同じく適用される。

6. PIVカード保有者の認証

本セクションでは、PIV カードによりサポートされる各種のアイデンティティ認証メカニズムと、アイデンティティ保証の累進的レベル一式に関する要件を満たす際にそれらのメカニズムを適用できるかどうかについて定義する。本セクションで述べる多様な認証メカニズムに加え、省庁および政府機関では、PIV カード上のアイデンティティクレデンシャルを使用するその他のメカニズムを採用してもよい（MAY）。PIV カードの文脈におけるアイデンティティ認証とは、PIV カードを提示するカード保有者の本人性に関する信用を確立するプロセスであると定義される。認証されたアイデンティティは、各種の物理リソースおよび論理リソースにアクセスするために当該個人に与えられる許可または権限を判定するために使用できる。

6.1 アイデンティティ認証の保証レベル

本規格では、PIV カードでサポートされるアイデンティティ認証について 3 段階の保証レベルを定義する。各保証レベルは、PIV カード保有者の本人性について確立される信用の程度を表す。認証を行う主体は、PIV カード保有者の本人性についての信用を次の事項に基づいて確立する。

1) PIV カードの発行に先立って実施されたアイデンティティの立証プロセスの厳格さ

2) PIV カードの発行および維持管理プロセスにおけるセキュリティ

3) カード保有者が当該 PIV カードの所有者であることの検証に使用される技術的メカニズムの強度

本規格のセクション 2 および 5 では、アイデンティティの立証および登録、身元証明の発行および維持管理の各プロセスに関してすべての PIV カードに必要とされる要件を定義している。したがって、これらのプロセスにおいては共通レベルの保証が存在する。PIV カードは視覚的および論理的な多数のアイデンティティクレデンシャルを保持する。カード保有者が当該 PIV カードの所有者であることを保証する保証のレベルは、何らかのリソースに対するアクセスを制御する主体に対し PIV カードの保有者を認証するために使用される具体的な PIV クレデンシャルに応じて異なる。この点を基準として、本規格では次のとおりアイデンティティ認証の保証レベルを定義する。

+ 「SOME Confidence」（ある程度の信頼性）－カード保有者の本人性が基礎的なレベルにおいて保証される

+ 「HIGH Confidence」（高い信頼性）－カード保有者の本人性が高度なレベルにおいて保証される

+ 「VERY HIGH Confidence」（非常に高い信頼性）－カード保有者の本人性が非常に高度なレベルにおいて保証される

連邦政府のリソース（物理的、論理的とも）に対するアクセス制御の責任を負う組織は、PIV カード保有者のアイデンティティ認証に誤りがあった場合に結果として個人や組織に生じる被害および影響に基づき、アクセスのために個人識別について必要とされる適切な保証レベルを決定しなければならない（SHALL）。必要な保証レベルが確定したら、PIV カード保有者の本人性に関して必要な程度の信用を確保するために、本セクションで規定する認証メカニズムを適用できる（MAY）。

6.1.1 OMBの電子認証ガイダンスとの関係

本規格でアイデンティティ認証について定義する各種の保証レベルは、OMB 発行の文書 M-04-04『E-Authentication Guidance for Federal Agencies（電子認証に関する連邦政府機関向けガイダン

ス）』[OMB404]セクション 2 の記述と密接に対応している。具体的には、PIV 保証レベルと[OMB404]で定められている保証レベルの間には表 6-1 に示す概念上の対応関係が存在する。

表 6 -1. PIV と電子認証ガイダンスにおける保証レベルの対応関係

OMB の電子認証レベル		対応する PIV 保証レベル
レベル番号	説明	
Level 2	主張されるアイデンティティの有効性についてある程度確実	SOME confidence（ある程度の信頼性）
Level 3	主張されるアイデンティティの有効性は信頼性が高い	HIGH confidence（高い信頼性）
Level 4	主張されるアイデンティティの有効性は信頼性が非常に高い	VERY HIGH confidence（非常に高い信頼性）

[OMB404]では「認証を必要とする電子的トランザクションのための本人性保証」を念頭に、アイデンティティ認証の誤りに関するリスクおよび考えられる影響に基づいて 1 つの方法論を規定している。PIV カードの文脈においては、論理リソースの所有者が、[OMB404]に規定される方法論を適用し、自身が行う電子的トランザクションに必要な保証レベルを特定しなければならない（SHALL）。物理リソースに対するアクセスに関して責任を負う組織では、[OMB404]の規定と同様の方法論を使用することで、当該の物理リソースに対するアクセスに必要な PIV の安全性レベルを判定できる（MAY）。また、その他の適切な方法論を使用することで、実際のアプリケーションにおける本人性保証に必要なレベルを判定できる（MAY）。

6.2 PIVカードの認証メカニズム

以降の各項では、PIV カードで提供される主要（必須）クレデンシャルセットによってサポートされる基本的な認証メカニズムの種類を定義する。本規格では、PIV カード上の必須でない（OPTIONAL）論理クレデンシャルの要素（対称認証鍵など）を使用して実装できる認証メカニズムについては定義しない。

PIV カードは、カードリーダが設置された環境とカードリーダがない環境の両方においてアイデンティティ認証に使用できる。カードリーダが存在する場合、これは接触型リーダと非接触リーダのいずれであってもよい。個々の状況に適用できる（MAY）PIV アイデンティティ認証メカニズムは、使用環境のパラメータに応じて異なる。

本セクションで説明するそれぞれの認証メカニズムは、出入管理ポイントから該当省庁または政府機関のネットワークインフラストラクチャに接続できる場合、バックエンドの証明書状態検証インフラストラクチャを使用してさらに強化することもできる。PIV 認証用証明書の状態は、当該カードに保持されたほかのクレデンシャル要素すべてと直接的に関連している。

6.2.1 PIVの視覚的クレデンシャルを使用した認証（VIS）

視覚による PIV カード保有者の認証は、物理的な施設およびリソースに対する出入管理をサポートする目的にのみ使用すること（SHALL）。

次のとおり、PIV カードの表側と裏側には視覚による識別および認証をサポートする必須の表示項目がある。

+ 写真
+ 氏名
+ 職員の身分識別情報
+ 有効期限
+ 連邦政府機関カードシリアル番号（裏側）
+ 発行元識別情報（裏側）

次の任意要素も PIV カード上に表示できる（MAY）。

+ 連邦政府機関または省庁の名称
+ 省庁または政府機関の印章
+ PIV カード保有者の身体的特徴
+ 申請者の署名

連邦政府の管理下にある施設の出入管理ポイントをカード保有者が通過しようとする際には、守衛員が、カード保有者の視覚的な識別検証と、識別された個人に当該出入管理ポイントの通過を許可すべきかどうかの判断を行う必要がある（SHALL）。視覚的な認証プロセスにおいて適用すべき（SHALL）一連の手順は次のとおりである。

1. 出入管理ポイントに配置された守衛は、PIV カードが真正であり、かつ一切の改変を加えられていないように見えることを確認する。
2. 守衛は、カード保有者の顔の特徴とカード上の写真を比較し、一致することを確認する。
3. 守衛は、カードが期限切れでないことを確認するため、カード上の有効期限をチェックする。
4. 守衛は、カード保有者の身体的特徴とカードに記載されている身体的特徴とを比較する（該当する場合（OPTIONAL））。
5. 守衛は、カード保有者の署名を採取し、カード上の署名と比較する（該当する場合（OPTIONAL））。
6. そのほか、カード上の 1 つ以上のデータ要素（氏名、職員の身分識別情報、連邦政府機関カードシリアル番号、発行元識別情報、政府機関名など）が、当該カード保有者にアクセスを許可すべきかどうかの判断に使用される。

以下に、視覚による認証メカニズムの特徴をいくつか示す。

+ 人手によるカード検査を要するため、アクセス制御を迅速または大量に処理することはできない
+ 改変が加えられていないカードを当該カード所有者以外が使用する場合の耐性は高い
+ 改ざんおよび偽造に対する耐性は低い
+ カードリーダが設置された環境、設置されない環境のいずれにも対応

6.2.2 PIV CHUIDを使用した認証

PIV カードには、CHUID と呼ばれる必須の論理クレデンシャルが格納される。4.2 項で述べたとおり、CHUID には多数のデータ要素が含まれる。

CHUID は、次の手順に従って PIV カード保有者の認証に使用されるものとする（SHALL）。

1. CHUID が PIV カードから電子的に読み出される。
2. 当該 CHUID が信頼できる機関によって署名されたものであり、かつ改変されていないことを確認するため、CHUID 上のディジタル署名がチェックされる（該当する場合（OPTIONAL））。
3. カードが期限切れでないことを確認するため、有効期限がチェックされる。
4. 1 つ以上の CHUID データ要素（FASC-N、政府機関コード、Data Universal Numbering System [DUNS]コードなど）が、当該カード保有者にアクセスを許可すべきかどうかを判断する承認チェックの入力として使用される。

以下に、CHUID による認証メカニズムの特徴をいくつか示す。

+ 迅速な認証処理により大量のアクセス制御に対応できる
+ 改変が加えられていないカードを当該カード所有者以外が使用する場合の耐性は低い
+ 接触型リーダ、非接触リーダのいずれにも対応

6.2.3 PIVバイオメトリックを使用した認証

PIV カードには、署名済みバイオメトリックが必須の要素として格納される。この情報は、カード保有者が提示する PIN を使用してカード保有者／カード間の（CTC：cardholder-to-card）認証を実行したあとにカードから読み出すことができる。PIV バイオメトリックは、カード外照合（match-off-card）方式によるカード保有者／外部システム間の（CTE：cardholder-to-external system）認証をサポートする目的で設計されている。以降の各項では、PIV バイオメトリックを利用する 2 種類の認証方式について定義する。

以下に、PIV バイオメトリック認証メカニズム（以降の説明を参照）の特徴をいくつか示す。

+ カード保有者との対話処理を 2 回必要とするため、メカニズムはほかより低速
+ PIN によるカード活性化を要するため、改変のないカードを当該カード所有者以外が使用する場合に対する耐性は高い
+ バイオメトリックがディジタル署名されており、これをチェックすることでメカニズムをさらに強化できる
+ 接触型カードリーダにのみ対応

6.2.3.1 PIVバイオメトリックを使用した無人認証（BIO）

PIV バイオメトリックによる無人認証は、次の手順に従って行うものとする（SHALL）。

1. CHUID がカードから読み出される。

2. カードが期限切れでないことを確認するため、CHUID 内の有効期限がチェックされる。

3. カード保有者に PIN の提示が要求され、PIV カードが活性化される。

4. PIV バイオメトリックがカードから読み出される。

5. 当該バイオメトリックが改変されておらず、かつ信頼できる情報源から発行されたものであることを確認するために、バイオメトリックのディジタル署名が検証される（該当する場合（OPTIONAL））。

6. カード保有者に現在のバイオメトリックサンプルの提示が要求される。

7. バイオメトリックサンプルがカードから読み出したバイオメトリックと一致する場合は、カード保有者が当該カードの所有者として認証される。

8. CHUID に含まれる FASC-N と、バイオメトリックの外部ディジタル署名に含まれる Signed Attributes フィールドの FASC-N とが比較される。

9. 1 つ以上の CHUID データ要素（FASC-N、政府機関コード、DUNS コードなど）が、当該カード保有者にアクセスを許可すべきかどうかを判断する承認チェックの入力として使用される。

6.2.3.2 PIVバイオメトリックを使用した有人認証（BIO-A）

PIV バイオメトリックによる有人認証は、次の手順に従って行うものとする（SHALL）。

1. CHUID がカードから読み出される。

2. カードが期限切れでないことを確認するため、CHUID 内の有効期限がチェックされる。

3. カード保有者に PIN の提示が要求される。PIN の入力は係員の監視下で行われること。

4. 提示された PIN を使用してカードが活性化される。PIV バイオメトリックがカードから読み出される。

5. 当該バイオメトリックが改変されておらず、かつ信頼できる情報源から発行されたものであることを確認するために、バイオメトリックのディジタル署名が検証される（該当する場合（OPTIONAL））。

6. カード保有者に現在のバイオメトリックサンプルの提示が要求される。バイオメトリックサンプルの掲示は係員の監視下で行われること。

7. バイオメトリックサンプルがカードから読み出したバイオメトリックと一致する場合は、カード保有者が当該カードの所有者として認証される。

8. CHUID に含まれる FASC-N と、バイオメトリックの外部ディジタル署名に含まれる Signed Attributes フィールドの FASC-N とが比較される。

9. 1 つ以上の CHUID データ要素（FASC-N、政府機関コード、DUNS コードなど）が、当該カード保有者にアクセスを許可すべきかどうかを判断する承認チェックの入力として使用される。

この認証メカニズムは、無人でのバイオメトリックによるクレデンシャルチェックとほぼ同様であるが、カード保有者による PIV カードの使用および PIN とバイオメトリックサンプルの掲示が、係員（守衛など）によって監視される点だけが異なる。

6.2.4 PIVの非対称暗号技術を使用した認証（PKI）

セクション 4 で述べたとおり、PIV カードには、非対称認証プライベート鍵および対応する証明書が必須の要素として格納される。PIV 非対称認証鍵による認証は、次の手順に従って行うものとする（SHALL）。

1. カード保有者に PIN の提示が要求される。
2. 提示された PIN を使用してカードが活性化される。
3. カードリーダからカードに対して、チャレンジ文字列が発行され、それに応答する非対称操作が要求される。
4. 先に発行されたチャレンジに対し、カードは、PIV 認証プライベート鍵を使用してそのチャレンジに署名し、関連付けられた証明書を添付することによって応答する。
5. 応答の署名に対する検証と、標準規格に準拠した PKI パス有効性確認が実施される。関連付けられているディジタル署名が、信頼できる情報源から発行されたものであることを確認するためにチェックされる。証明書の現在の有効性を確認するために失効状態がチェックされる。
6. 応答が、発行されたチャレンジに対して期待されるとおりの内容かどうか検証される。
7. 認証用証明書から Subject Distinguished Name と FASC-N が抽出され、承認関数への入力として引き渡される。

以下に、PKI による認証メカニズムの特徴をいくつか示す。

+ オンラインで証明書状態チェックを実行するインフラストラクチャが必要
+ クレデンシャルの偽造に対する耐性は高い
+ PIN によるカード活性化を要するため、改変のないカードを当該カード所有者以外が使用する場合に対する耐性は高い
+ 接触型カードリーダに対応

6.3 アイデンティティ認証用の段階的な保証レベルに関するPIVのサポート

PIV カードでは、アイデンティティ認証用の段階的な保証レベルの実装に使用できる複数の認証メカニズムがサポートされている。6.1 項で定義したアイデンティティ認証の保証レベルをサポートする目的に使用できる（MAY）基本的な PIV 認証メカニズムについて、以降の各項で指定する。基本的なアイデンティティ認証メカニズムのうち 2 つ以上を併用することもでき、そうすることで PIV カード保有者の本人性をより高いレベルで保証できる（MAY）。

6.3.1 物理的なアクセス

PIV カードは、物理的なアクセス制御環境においてカード保有者の認証に使用できる。たとえば、連邦政府の施設には、チェックポイントに守衛を配置した物理的な出入口や、電子的な出入管理ポイントが存在する場合がある（MAY）。物理的なアクセス制御システム向けに PIV カードでサポートされる認証メカニズムの要約を表 6-2 に示す。高い保証レベルに適した認証メカニズムは、それよりも低い保証レベルの要件にも対応可能であるが、これについては明示していない。

この表に示すそれぞれの認証メカニズムは、出入管理ポイントから該当省庁または政府機関のネットワークインフラストラクチャに接続できる場合、バックエンドの証明書状態検証インフラストラクチャを使用してさらに強化することもできる。

表 6 -2. 物理アクセス用の認証

用途／リソースに必要とされる PIV 保証レベル	適用可能な PIV 認証メカニズム
SOME confidence（ある程度の信頼性）	VIS、CHUID
HIGH confidence（高い信頼性）	BIO
VERY HIGH confidence（非常に高い信頼性）	BIO-A、PKI

6.3.2 論理的なアクセス

PIV カードは、論理的な情報リソースに対するアクセスの判定をサポートする目的で、カード保有者の認証に使用できる（MAY）。たとえば、カード保有者が自身の所属する省庁または政府機関のネットワークに PIV カードを使用してログインした場合、その認証プロセスによって確認された本人性は、当該ネットワーク上で利用可能なファイルシステム、データベース、その他サービスに対するアクセスの可否を判定するために使用できる（MAY）。

表 6-3 に、本規格のために定義された、論理アクセス制御をサポートする認証メカニズムの説明を示す。高い保証レベルに適した認証メカニズムは、それよりも低い保証レベルの要件にも対応可能であるが、これについては明示していない。

表 6 -3. 論理アクセス用の認証

用途／リソースに必要とされる PIV 保証レベル	適用可能な PIV 認証メカニズム	
	ローカルワークステーション環境	リモート／ネットワークシステム環境
SOME confidence（ある程度の信頼性）	CHUID	PKI
HIGH confidence（高い信頼性）	BIO	
VERY HIGH confidence（非常に高い信頼性）	BIO-A、PKI	

付録A—PIVのプロセス

本規格の 2.2 項および 5.2 項では、アイデンティティの立証および登録に関して承認されたプロセスを採用および運用することを義務付けている。アイデンティティの立証および登録システムはすべて、この承認を受けるために、2.2 項および 5.2 項に示す PIV の目標および要件を満たさなければならない（MUST）。

本規格の 2.3 項および 5.3 項では、クレデンシャルの発行および維持管理に関して承認されたプロセスを採用および運用することを義務付けている。クレデンシャルの発行および維持管理システムはすべて、この承認を受けるために、2.3 項および 5.3 項に示す PIV の目標および要件を満たさなければならない（MUST）。連邦政府省庁および政府機関の長は、必須とされる PIV の目標および要件を満たすことが認定されたアイデンティティの立証、登録および発行プロセスに関して、使用を承認できる（MAY）。

必須とされる PIV の管理目標およびセキュリティ要件を満たす PIV アイデンティティの立証、登録および発行プロセスについて、本付録に 2 つの例を示す。PIV-II の目標を満たすために追加的な PIV-II 要件が必要となる箇所では、随時その旨が指定されている。

A.1 ロールベースのモデル

ロールベースでのアイデンティティの立証、登録および発行プロセスは、既存の PIV システムを持たない組織において推奨される（RECOMMENDED）。

A.1.1 PIVアイデンティティの立証および登録

PIV クレデンシャルの発行に関して汎用的なプロセスセットを採用する省庁および政府機関は、本セクションで定義するアイデンティティの立証および登録プロセスに従うこと（SHALL）。

A.1.1.1 役割（ロール）および責務

PIV アイデンティティの立証、登録および発行プロセスに関連付けられる重要な役割は以下に定義するとおりである。これらの役割は、別の主たる任務を負う職員に対して付加的に割り当てることができる（MAY）。アイデンティティの立証および発行に関しては次の役割を採用すること（SHALL）。

+ 申請者（Applicant）－PIV クレデンシャルの発行対象となる個人。
+ PIV 保証人（PIV Sponsor）－申請者に対する PIV クレデンシャルの発行が必要であることを証明し、申請者についての保証を提供する個人。申請者に対する PIV クレデンシャルの発行を要求する。
+ PIV 登録機関（PIV Registrar）－申請者のアイデンティティの立証および身元調査の完遂に関して責任を負う主体。申請者に対する PIV クレデンシャルの発行について最終的な承認を行う。
+ PIV 発行元（PIV Issuer）－クレデンシャルのパーソナライゼーション操作を実施し、また、すべてのアイデンティティの立証、身元調査および関連する承認処理が完了したあとにクレデンシャルを発行する主体。また、PIV 発行元は、PIV クレデンシャルストックに関する記録と制御の維持管理について責任を負い、正当なクレデンシャルを発行する以外の目的にストックが使用されることのないようにする。

+ PIV ディジタル署名機関（PIV Digital Signatory）－PIV バイオメトリックおよび CHUID に対してディジタル署名を行う主体。この役割は PIV-II にのみ適用される。

+ PIV 認証 CA（PIV Authentication Certification Authority）－PIV 認証用証明書を署名および発行する認証局。この役割は PIV-II にのみ適用される。

PIV 申請者、保証人、登録機関、発行元の各役割は相互に排他的である。すなわち、アイデンティティの立証および登録プロセス内において、いかなる個人もこれらのうち複数の役割を割り当ててはならないものとする（SHALL）。PIV 発行元および PIV ディジタル署名機関の役割については、単一の個人または機関が両方を兼ねることができる（MAY）。PIV 認証 CA は、5.4.1 項で指定するとおり共通ポリシー（Common Policy）に基づいて証明書を発行することを認定された CA である。

PIV 登録機関、発行元、ディジタル署名機関の各役割は、何らかの公式な認定プロセスにより確立される該当要件を満たすものとする（SHALL）。

A.1.1.2 新規の職員および委託業者のアイデンティティの立証および登録

申請者は、連邦政府で雇用されるための審査プロセスの一環として、または、連邦政府の管理下にある物理的施設や情報リソースへのアクセスを求めるために、PIV クレデンシャルを申請する。本文書の本項では、アイデンティティソース文書の検査と身元調査によって個人識別の保証を確立するための 1 つのプロセスを定義する。このプロセスは、PIV アイデンティティクレデンシャルについて均一レベルの保証を確保するために最低限必要な機能要件およびセキュリティ要件を提供するものである。実際のプロセスが本項で規定する要件を満たす限りにおいて、発行元となる組織は、当該組織に特有の要件を満たすためにプロセスを強化または拡張してよい（MAY）。アイデンティティの立証と登録に関する要件には次の事項を含むものとする（SHALL）。

+ PIV 保証人は、特定の申請者 1 人につき PIV 申請書 1 通を作成し、これを PIV 登録機関および PIV 発行元に提出するものとする（SHALL）。PIV 申請書は次の項目を含むものとする（SHALL）。

  - PIV 保証人の氏名、組織および連絡先情報（保証組織の所在地を含む）
  - 申請者の氏名、生年月日、身分および連絡先情報
  - 指定 PIV 登録機関の名称および連絡先情報
  - 指定 PIV 発行元の名称および連絡先情報
  - PIV 保証人の署名

  PIV 登録機関は、PIV 申請書の受理に先立ってその正当性を確認しなければならない（SHALL）。

+ 申請者は、必須とされる背景情報を提供するために OPM の Standard Form (SF) 85「Questionnaire for Non-Sensitive Positions（取り扱いに注意を要しない身分についての質問事項）」または同等のフォームを記入するものとする（SHALL）。申請者は、この背景情報フォームを完成して PIV 登録機関に提出するものとする（SHALL）。

+ 申請者は本人が出頭し、アイデンティティソース文書 2 種類の原本を提出すること（SHALL）。アイデンティティソース文書は、「Form I-9, OMB No. 1115-0136, Employment Eligibility Verification（採用適格性検査）」に含まれている受理可能文書一覧に属するものでなければならない（MUST）。文書の少なくとも 1 つは連邦政府または州政府によって発行された写真付きの有効な身分証明書であるものとする（SHALL）。PIV 登録機関は、アイ

デンティティソース文書を視覚的に検査し、これが真正かつ改変されていないことを認証すること（SHALL）。また、アイデンティティソース文書の信ぴょう性を電子的に検証する手段が当該文書の発行元から提供されている場合、PIV 登録機関はこの検証を実行すること（SHALL）。電子的な検証手段が提供されない場合、PIV 登録機関はその他の利用可能な手段によって、アイデンティティソース文書の出所および保全性を認証すること（SHALL）。その後、PIV 登録機関はアイデンティティソース文書に表示された写真と申請者とを比較し、申請者が当該アイデンティティソース文書の保有者であることを確認すること（SHALL）。以上すべてのチェックにおいて問題がないと認められる場合、PIV 登録機関は、提示された 2 種類のアイデンティティソース文書それぞれについて次のタイプのデータを記録し、当該記録に署名したうえでファイルに保管すること（SHALL）。

- 文書のタイトル
- 文書の発行元機関
- 文書の番号
- 文書の有効期限（該当する場合（OPTIONAL））
- その他、申請者の本人性確認に使用したすべての情報

+ PIV 登録機関は、PIV 申請書に記載された申請者情報（フルネーム、生年月日、連絡先情報など）と、申請者により提示された対応する情報とを比較すること（SHALL）。

+ PIV 登録機関は、申請者の顔写真画像を採取し、この画像のコピーをファイルに保管すること（SHALL）。PIV-II において顔写真画像を採取する場合は、[SP800-76]に基づく顔写真画像の仕様に適合する画像であること（SHALL）。

+ PIV 登録機関は、申請者の指紋押捺を行い、4.4 項の定義に従い申請者のすべての指紋を採取して、そのコピーを保管すること（SHALL）。また、PIV-II においては、4.4 項に従って申請者の指紋 2 つを電子的形式で採取すること（SHALL）。

+ PIV 登録機関は、大統領行政命令 10450 [EO10450]によって要求されるとおり、NACI を申請者に対して開始すること（SHALL）。付録 C に、NACI および NAC の詳細を示す。この調査により何らかの望ましくない結果が得られた場合は、当該申請者が PIV クレデンシャルの取得に適格かどうかを判定するため、当該結果について裁定を下すこと（SHALL）。

+ 上記すべての要件が完了した場合、PIV 登録機関は保証人および PIV 発行元に対し、当該申請者への PIV クレデンシャルの発行が承認された旨を通知すること（SHALL）。逆に、必要とされる手順のいずれかにおいて問題が生じた場合、PIV 登録機関はこれらの機関に対し適切な通知を送付すること（SHALL）。

+ PIV 登録機関は PIV 発行元に対し、安全なプロセスによって次の情報を提供すること（SHALL）。

  - 申請者の顔写真画像
  - 申請者の身元調査結果のコピー
  - 申請者に関するその他のデータ（職員の身分など）

+ PIV-II においては、PIV 登録機関は PIV ディジタル署名機関に対し、安全なプロセスによって次の情報を提供すること（SHALL）。

- カードのパーソナライゼーションに使用する電子的バイオメトリックデータ
- カードのパーソナライゼーションに使用する署名済みオブジェクトの生成に必要な、申請者に関するその他のデータ

+ PIV 登録機関は次の事項の維持管理について責任を負うものとする（SHALL）。
  - 記入および署名済みの PIV 申請書
  - 申請者から提出された、記入および署名済みの SF 85 フォーム（または同等のフォーム）
  - チェック済みのアイデンティティソース文書に関する情報
  - 必須の身元調査の結果
  - 顔写真画像および指紋のコピー
  - その他、申請者の本人性保証に使用したすべての材料

上記データの維持管理に使用される格納およびアクセス制御メカニズムの実装においては、2.3 項で指定するプライバシポリシーを含め、セキュリティ、プライバシ、記録保管に関して該当するすべての連邦政府規制に従わなければならない（SHALL）。

A.1.1.3 現行の職員および委託業者に対するアイデンティティの立証および登録

現行の職員および委託業者に対して PIV クレデンシャルを発行または再発行する場合は、A.1.1.2 項で説明したアイデンティティの立証プロセスに従うこと（SHALL）。ただし、PIV 登録機関が申請プロセスにおいて身元調査の結果を参照し、確認できる場合には、身元調査の実施は不要である（NOT REQUIRED）。

A.1.2 PIV発行

PIV クレデンシャルの発行プロセスは、以下に定義する機能上およびセキュリティ上の要件を満たさなければならない（SHALL）。発行プロセスは、各省庁および政府機関に特有の制約および要件に応じて拡張することもできる（MAY）。ただし、拡張した実際のプロセスは本項で規定する要件を満たさなければならない（SHALL）。

+ PIV 発行元は、保証人から受け取る PIV 申請書および PIV 登録機関から受け取る承認通知の正当性を確認するものとする（SHALL）。また、PIV 発行元は、承認通知の内容が身元調査の結果に合致することを確認しなければならない（SHALL）。
+ PIV 発行元は、PIV 登録機関から提供される情報に基づく新規 PIV クレデンシャルの作成および個人情報設定を管理するものとする（SHALL）。PIV-II においては、PIV 発行元によって新規 PIV クレデンシャルの CHUID 作成が開始されるものとする（SHALL）。この CHUID を、安全なメカニズムを介して PIV ディジタル署名機関が利用できるようにしなければならない（SHALL）。
+ PIV-II の場合、ディジタル署名機関が、PIV 登録機関から提供されるデータと、新規に割り当てられる CHUID を使用して、カードのパーソナライゼーションプロセスに必要なディジタル署名済みクレデンシャル要素（バイオメトリックおよび CHUID）を作成するものとする（SHALL）。ディジタル署名済みクレデンシャル要素は、4.2.2 項および 4.4.2 項の該当する

仕様に適合しなければならない（SHALL）。署名済みクレデンシャルの要素は PIV 発行元に対して利用可能とされなければならない（SHALL）。

+ 申請者が PIV クレデンシャルを受け取るには、申請者本人が PIV 発行元（または認可された委任先）に出頭しなければならない（SHALL）。新規に作成した PIV クレデンシャルの申請者への引き渡しに先立ち、PIV 発行元は次の手順により、身元証明を受け取る個人が確かに申請者であることを確認しなければならない（SHALL）。

  − 出頭した個人に、州または連邦政府から発行された写真入りのアイデンティティソース文書を提示させる（SHALL）。PIV 発行元（または認可された委任先）は、当該情報源文書に表示された写真および氏名と、パーソナライズしようとしている新規 PIV クレデンシャルに表示される写真および氏名との一致を検証すること（SHALL）。また、PIV 発行元（または認可された委任先）は、出頭した個人の身体的特徴と当該 PIV クレデンシャルに印刷されようとしている写真との一致を検証すること（SHALL）。

  − PIV-II の場合、PIV 発行元（または認可された委任先）は、出頭した個人の指紋と PIV 身元証明に組み込まれるバイオメトリッククレデンシャルとの一致も確認する（SHALL）。

+ PIV-II の場合、PIN の提示を申請者に要求するか、または PIV 発行元が申請者のために PIN を生成する（MAY）。

+ PIV 発行元は PIV クレデンシャルをパーソナライズするものとする（SHALL）。パーソナライズした PIV クレデンシャルは、PIV-II の要件に適合するために、セクション 4 の技術仕様および相互運用性に関する仕様すべてを満たさなければならない（SHALL）。

+ PIV-IIの場合、申請者は当該PIVクレデンシャルのための暗号鍵ペアを生成し、この時点で、対応する証明書をPIV認証CAから取得することができる（MAY）。または、1 回限り有効な認証手段 [7] が申請者に提供され、申請者はこれを使用してPIV認証CAに証明書を要求する場合もある（MAY）。後者の場合、申請者は、PIV発行元においてではなくローカルワークステーション [8] において鍵ペアを生成する。

+ PIV-II の場合、受取人名、発行元識別情報、カード番号、および（該当する場合（OPTIONAL））PKI 証明書識別情報が、PIV システムをサポートするバックエンドのデータ格納域に登記および登録されるものとする（SHALL）。インフラストラクチャの設計に応じて、バックエンドのデータ格納域は集中型であっても分散型であってもよい（MAY）。

+ PIV 発行元（または認可された委任先）は、申請者（PIV クレデンシャル保有者となった個人）から、PIV クレデンシャルおよび付随する責任を受け入れたことを証明する署名を取得するものとする（SHALL）。

+ 上記すべての要件が完了した場合、PIV 発行元は PIV 保証人および指定された PIV 登録機関に対し、パーソナライゼーションおよび発行プロセスが完了した旨を通知するものとする（SHALL）。逆に、必要とされる手順のいずれかにおいて問題が生じた場合、PIV 登録機関はこれらの機関に対し適切な通知を送付すること（SHALL）。

+ PIV 発行元は次の事項の維持管理について責任を負うものとする（SHALL）。

  − 記入および公式に認可済みの PIV 申請書

---

7 発行元機関は、必要な PKI 管理機能がサポートされており、[COMMON] において義務付けられているセキュリティポリシー目標に適合するように実装されていることを保証しなければならない。

8 発行元機関は、必要な PKI 証明書の管理の責任を負う。

- PIV 登録機関からの承認通知
- PIV クレデンシャル保有者（申請者）の名前
- 身元証明書の識別情報。PIV-II の場合、連邦政府機関カードシリアル番号がこの識別情報に該当する
- PIV クレデンシャルの有効期限
- PIV クレデンシャル保有者による受け入れの署名

上記データの維持管理に使用される格納およびアクセス制御メカニズムの実装においては、2.4 項で指定するプライバシポリシーを含め、セキュリティ、プライバシ、記録保管に関して該当するすべての連邦政府規制に従わなければならない（SHALL）。

A.2 システムベースのモデル

自動化されたアイデンティティ管理システムを持つ組織では、システムベースのアイデンティティ立証、登録および発行のプロセスセットを採用できる（MAY）。本項は、政府のスマートカードに関する省庁間諮問委員会（Government Smart Card Interagency Advisory Board）より提供されたものである。

A.2.1 PIVアイデンティティの立証および登録

本規格の 2.2 項および 5.2 項に示す PIV の管理目標に適合するため、自動化されたアイデンティティ管理システム(Automated Identity Management System)によるシステムベースのアイデンティティの立証、登録および発行のプロセスセットを採用する政府機関は最低限、PIV クレデンシャルの発行時に、A2.1 項から A2.4 項で定義するアイデンティティ検証および登録プロセスに従わなければならない（SHALL）。図 A-1「PIV アイデンティティの検証および発行」に、PIV アイデンティティの立証およびクレデンシャルの発行プロセスを構成する論理的構成要素を示す。この図は、PIV の管理目標および要件をサポートするために最低限必要とされる必須の要素および役割を示すものである。

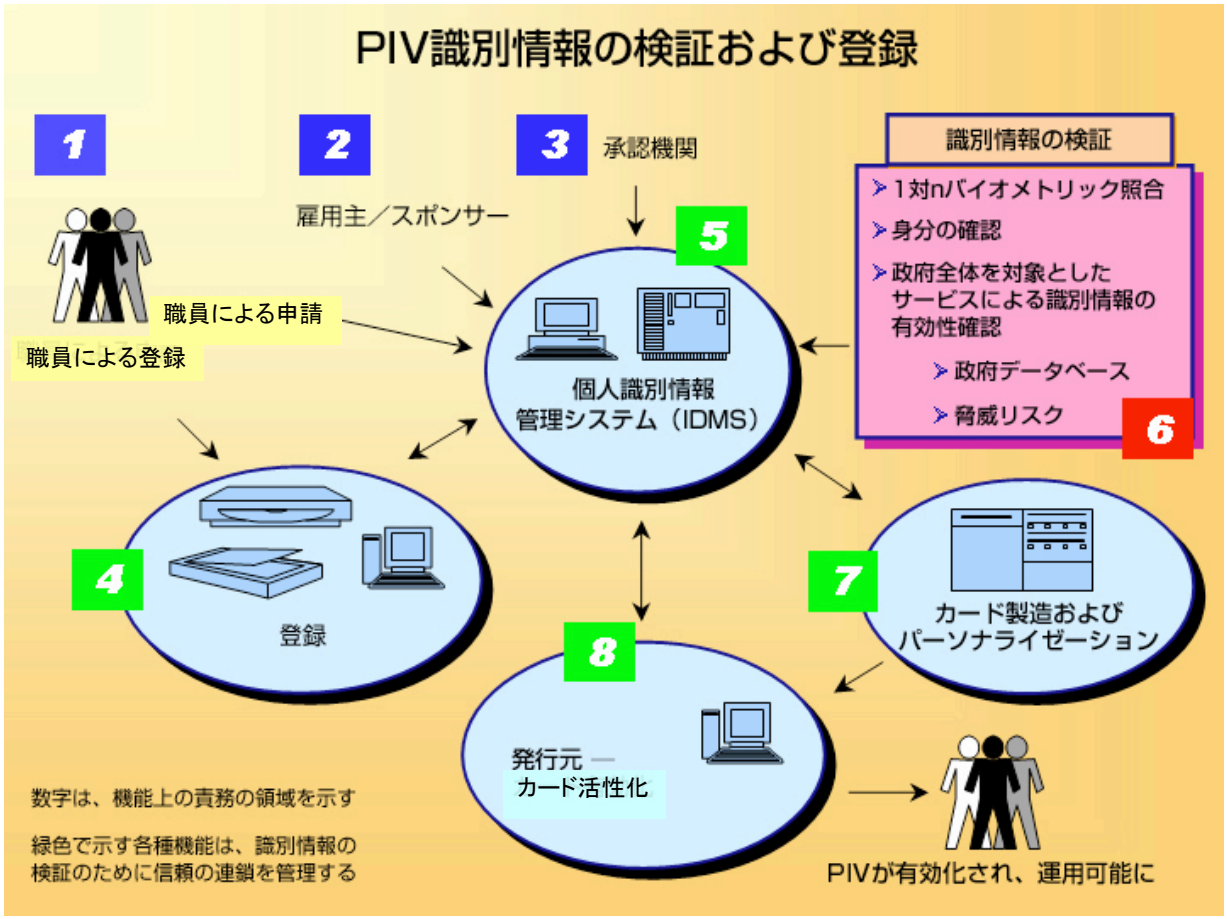


図 A-1. PIV アイデンティティの検証および登録

A.2.2 役割および責務

システムベースの PIV アイデンティティ立証、登録および発行のプロセスに関連付けられる役割は以下に定義するとおりである。

+ 申請者（Applicant）－PIV クレデンシャルの発行対象となる個人。主張する本人性を証明するために必要なアイデンティティソース文書を提示するものとする（SHALL）。
+ 雇用主（Employer）／保証人（Sponsor）－申請者との関係を証明し、申請者についての保証を提供する個人。雇用主／保証人は PIV クレデンシャルの申請を認可する（SHALL）。
+ 登録担当（Enrollment Official）－アイデンティティの立証のために信頼の連鎖（chain of trust）の起点となり、雇用主による保証の確認、申請者とそのバイオメトリックとの関連づけ、およびアイデンティティソース文書の検証について信頼できるサービスを提供する個人。裁決用のアイデンティティ管理システム（IDMS：Identity Management System）に対して安全な登録パッケージを提供する。
+ 承認機関（Approval Authority）－PIV 申請承認用の IDMS 内で組織的な命令系統を確立する主体。これには、承認済みの雇用主／保証人の確立も含まれる。記入された PIV 申請に対する自動または手動での承認プロセスを指定できる（MAY）。機能プロセスにおいて確立される信頼の連鎖について、その全体を管理する（SHALL）。適切なプライバシ管理策およびセキュリティ管理策を管理する（SHALL）。

+ 発行機関（Issuing Authority）／発行元（Issuer）－すべてのアイデンティティの立証、身元調査および関連する承認処理が完了したあとに申請者に対して PIV クレデンシャルを発行する主体。

発行元は、PIV 登録レコードに照らして申請者の 1 対 1 のバイオメトリック照合を行うことにより、信頼の連鎖を完成するものとする（SHALL）。本人性が正しく確認されたら、発行元はカードを活性化する（SHALL）。そのあと、当該個人に対してクレデンシャルを発行する（SHALL）。

役割は、いずれか 1 つの役割を組織内の単一の個人が担当することを義務付けるために定義されるものではない。すべての役割およびプロセスは、本規格に適合する認定されたサービスプロバイダが提供してよい（MAY）。

承認機関は、ベストプラクティスに従い、リスクに応じて役割および責務の分担を決定するものとする（SHALL）。承認機関は信頼の連鎖プロセスにおいて少なくとも 2 名の人員がそれぞれ異なる機能を実施していることを保証しなければならない（SHALL）。特定の個人が、認可された別の個人の協力なしに単独で PIV クレデンシャルを発行できないことを保証する、業務分割の原則に従うこと（SHALL）。カードの製造は、カードストック管理に関してセキュリティ目標および品質管理目標が完全に満たされる限りにおいて、中央のカード発行施設または離れたカード発行施設のいずれで行われてもよい（MAY）。PIV カードの発行の前に、申請者本人が少なくとも一度は出頭しなければならない（MUST）。

PIV アイデンティティの立証および発行プロセスに関連する構成要素は次のとおりである。

+ アイデンティティ管理システム（IDMS）－承認機関は、発行済み PIV クレデンシャルの記録システムである IDMS を維持管理しなければならない（SHALL）。IDMS は、主張される身元の有効性を確認するためのアイデンティティの立証、検証および妥当性確認を実行するものであり、同一の申請者が複数の名前で登録されないようにするための 1 対多照合機能を提供する（SHALL）。職員の身分が PIV 申請に適切であるかどうかを確認する（SHALL）。アイデンティティの有効性確認および検証サービスを、HSPD-11 に従って提供される政府全体を対象とした標準化されたサービス（6 種類）を通して管理する（SHALL）。主張される本人性に対する裁定を管理する（SHALL）。主張される本人性が認められたら、申請者に対する PIV の発行を承認する（SHALL）。

+ 登録システム（Enrollment System）－アイデンティティの立証のために信頼の連鎖の起点となる。登録担当は、雇用主による保証の確認、申請者とそのバイオメトリックとの関連づけ、および主張される本人性を証明する文書の検証について信頼できるサービスを提供しなければならない（SHALL）。登録担当により、裁決用の IDMS に対して安全な登録パッケージが提供される。

+ カード製造およびパーソナライゼーションシステム（Card Production and Personalization System）－IDMS の承認に基づいて PIV クレデンシャルを印刷およびパーソナライズするための、完全に在庫管理されたプロセスを提供する（SHALL）。空白カードのストック、およびパーソナライズ／印刷後の活性化前カードのストックについて、状態の追跡、在庫の管理、および保護のためのメカニズムを提供する（SHALL）。

PIV アイデンティティの立証および発行に関する要件およびワークフローは次のとおりである。

+ 申請者（Applicant）－アイデンティティクレデンシャルの発行対象となる個人。主張する本人性を証明するために登録用のアイデンティティソース文書を提示する（SHALL）。

+ 雇用主（Employer）／保証人（Sponsor）－申請者との関係を証明し、申請者についての保証を提供する（SHALL）。PIV クレデンシャルの申請を認可する（SHALL）。

+ 承認機関（Approval Authority）－図 A-2 の 4 から 8 に該当する機能プロセス領域において確立される信頼の連鎖について、全体の管理に責任を負う（SHALL）。

+ 登録担当（Enrollment）－アイデンティティの立証のために信頼の連鎖の起点となる。登録担当は、雇用主による保証の確認、申請者とそのバイオメトリックとの関連づけ、および主張される本人性を証明する文書の検証について信頼できるサービスを提供しなければならない（SHALL）。登録担当により、裁決用の IDMS に対して安全な登録パッケージが提供される。

+ アイデンティティ管理システム（IDMS）－承認機関は、当該機関の発行した PIV クレデンシャルの記録システムである IDMS を維持管理しなければならない（SHALL）。IDMS は、主張される身元の有効性を確認するためのアイデンティティの立証、検証および妥当性確認を実行するものであり、同一の申請者が複数の名前で登録されないようにするための照合機能を提供する（SHALL）。職員の身分が PIV 申請に適切であるかどうかを確認する（SHALL）。アイデンティティの有効性確認および検証サービスを、HSPD-11 に従って提供される政府全体を対象とした標準化されたサービス（6 種類）を通して管理する（SHALL）。主張される本人性に対する裁定を管理する（SHALL）。主張される本人性が認められたら、申請者に対する PIV の発行を承認する（SHALL）。

+ カード製造およびパーソナライゼーション（Card Production and Personalization）－IDMS の承認に基づいて PIV クレデンシャルを印刷およびパーソナライズするための、完全に在庫管理されたプロセスを提供する（SHALL）。空白カードのストック、消耗品、およびパーソナライズ／印刷後の活性化前カードのストックについて、保護のためのメカニズムを提供する（SHALL）。

+ 発行元（Issuer）－すべてのアイデンティティの立証、身元調査および関連する承認処理が完了したあとに申請者に対してアイデンティティクレデンシャルを発行する主体。信頼の連鎖を、申請者と PIV 登記記録との 1 対 1 バイオメトリック照合の実行、および登録レコードの写真と申請者との一致検証によって完成する（SHALL）。本人性が正しく確認されたら、発行元はカードを活性化する（SHALL）。活性化をもって、発行元は当該個人のバイオメトリックを PIV クレデンシャルに照らして検証し、信頼の連鎖を完結する（SHALL）。そのあと、当該個人に対してクレデンシャルを発行する（SHALL）。

A.2.3 アイデンティティの立証および登録

このプロセスに関与する者すべてによる、要求に対する承認／拒否のために行われるすべての行為は、犯罪捜査およびシステム管理の両方をサポートし得る、監査可能な証跡を残さなければならない（SHALL）。この監査証跡により、PIV の発行と管理のための信頼の連鎖に関する重要な管理要素が提供されるものとする（SHALL）。

A.2.4 雇用主／保証人

雇用主／保証人は、前もって IDMS に登録されていることが必要である（MUST）。承認機関には、雇用主／保証人のための役割を確立する必要がある（MUST）。雇用主／保証人は政府の組織であっても、委託業者の組織であってもよい（MAY）。承認機関は、申請者から提出される PIV 申請の承認に関して適切な権限を雇用主／保証人に委任するものとする（SHALL）。

A.2.5 PIVの申請プロセス

PIV の申請プロセスは次の 4 つの要素から構成される。

1. 申請者が、PIV の要求とその主張する本人性を証明する文書とを提出する
2. 雇用主／保証人が、申請者の要求を承認する
3. 承認機関が、PIV 申請および適切な保証を確認および承認し、PIV の要求を承認する（SHALL）
4. 登録担当が、(1)、(2)、(3)からの提出物を結合して公式の IDMS 向け提出物とし、アイデンティティの検証および有効性確認プロセスを開始する

申請者は、PIV の公式な申請を提出しなければならない（SHALL）。

雇用主／保証人は、申請者の要求を承認するものとする（SHALL）。

雇用主の保証および承認を得たあと、申請者は登録のために出頭するものとする（SHALL）。申請者は、Form I-9, OMB No. 1115-0136「Employment Eligibility Verification（採用適格性検査）」の受理可能文書一覧に記載されている身分証明書のうち少なくとも 2 種類を PIV 登録機関に提示しなければならない（SHALL）。提示する文書のうち少なくとも 1 つは、連邦政府または州政府によって発行された写真付きの有効な身分証明書でなければならない（SHALL）。

A.2.6 PIV登録プロセス

PIV 登録プロセスにおける最小限の手順は次のとおりとする（SHALL）。

1. 申請者が、証明用の文書を持参して登記のために出頭する（SHALL）
2. 登録担当が、自動化された手段が利用可能な場合はこれを使用し、証明用の文書をすべて検査および確認する（SHALL）
3. 登録担当が、出頭した個人と証明用の文書との一致を確認する（SHALL）
4. 登録担当が、PIV に対する雇用主／保証人の承認を確認する（SHALL）
5. 登録担当が、証明用の文書すべてをスキャンする（SHALL）

PIV 結合プロセスにおける最小限の手順は次のとおりとする（SHALL）。

1. 登録担当が、申請者のバイオメトリックサンプルおよび写真を採取する（SHALL）
2. 登録担当が、バイオメトリックおよび写真の採取に関する品質保証プロセスを管理する（SHALL）。バイオメトリックサンプルについては正しい性能が得られることを確認しなければならない（SHALL）
3. 登録担当が、完成した電子的登録パッケージをディジタル署名と結合し、この登録申請をアイデンティティの検証および有効性確認のために IDMS に転送する（SHALL）

完成した PIV 登録パッケージには次の内容が含まれるものとする（SHALL）。

+ 主張される本人性を証明する文書のスキャン
+ バイオメトリックサンプルおよびディジタル写真画像
+ 個人の経歴および組織に関する情報
+ 登録担当のディジタル署名

A.2.7 アイデンティティの検証プロセス

IDMS は、PIV 用の完成したパッケージを登録担当から受け取るものとする（SHALL）。IDMS ではこのパッケージの完全性、正確性およびディジタル署名を確認することにより、パッケージの完全性を検証するものとする（SHALL）。

IDMS は、パッケージ内に明示された職員の身分および保証人の情報を確認する手段を提供するものとする（SHALL）。

IDMS は、パッケージ内に明示された個人から以前に別の名前で申請が行われていないことを保証するために 1 対多照合を実行するものとする（SHALL）。

IDMS は HSPD-11 に従い、政府全体を対象としたデータベースおよびサービスを使用して、適切なアイデンティティの検証および有効性確認を実施するものとする（SHALL）。

承認機関は、これら 3 種類の主要なチェックにおいて潜在的なリスクが発見された場合、主張される本人性に対して裁定を下すものとする（SHALL）。

適切なアイデンティティ検証プロセスが正常に完了した場合、承認機関は、当該クレデンシャルに対するカード製造を承認するものとする（SHALL）。アイデンティティを検証および有効性確認するための主要なチェックすべてに要する期間が 10 日を超える場合、承認機関は、それらの完了に先立って PIV クレデンシャルの発行を承認してもよい（MAY）。

IDMS は次の事項の維持管理について責任を負うものとする（SHALL）。

1. 記入および署名済みの PIV 登録パッケージ
2. アイデンティティソース文書のコピー
3. 申請者から提出された、記入および署名済み経歴情報フォーム
4. 必須の身元調査の結果
5. その他、申請者の本人性保証に使用したすべての材料
6. アイデンティティクレデンシャルのシリアル番号など、クレデンシャルのアイデンティティ
7. アイデンティティクレデンシャルの有効期限
8. 承認された申請者ごとに固有の最小限のアイデンティティレコード
9. 登録時に採取されたバイオメトリックデータの原本を格納する、最小限のアイデンティティレコードにより索引付けされた別個のデータベース。これらのデータは安全のため暗号化すること（SHALL）

10. バイオメトリックデータを管理する別個のデータベース。最小限のアイデンティティレコードにより索引付けされ、指紋自動識別システム（AFIS：Automated Fingerprint Identification System）のために 1 対多のアイデンティティチェックをサポートする

IDMS は次の機能を備えたサービスを提供するものとする（SHALL）。

1. 申請者である職員／委託業者に PIV の状態を通知する機能
2. 雇用主に PIV の状態を通知する機能
3. 発行済みクレデンシャルが現在有効かどうかを任意の他者が照会できる有効性確認機能

IDMS は、サポート対象であるカード製造施設の要求に応じ、すべての承認済み PIV クレデンシャルについて、カード製造用の完全なパーソナライゼーション情報および印刷情報を提供するものとする（SHALL）。この情報は、対象個人、発行元、実行されるアイデンティティ検証、クレデンシャル、およびバイオメトリックの間に完全な信頼の連鎖の成立を可能にするために提供されるものとする（SHALL）。

A.2.8 カードの製造、活性化および発行

カードの製造は、中央の施設または離れた場所の施設のいずれで行われてもよい（MAY）。IDMS は、PIV クレデンシャルのライフサイクル全体、すなわち最初の製造要求からパーソナライゼーションおよび印刷、活性化および発行、利用の中断、失効および廃棄に至るまでの全期間を通じて常にその状態を把握していなければならない（SHALL）。

カードの製造サービスは次の能力を備えなければならない（SHALL）。

1. 初期化された空白カードまたは（たとえば、製造元の鍵を使って）事前発行されたカードのストック、消耗品、および製造材料について、完全な在庫管理を維持する
2. カード製造の PIV 要求を送出できる承認済みの IDMS システムの一覧を維持管理する
3. PIV 製造の IDMS 要求に対して確認応答を返す
4. PIV クレデンシャルの製造完了を IDMS に通知する
5. PIV クレデンシャルを活性化および発行できる承認済みの発行元の一覧を維持管理する
6. PIV クレデンシャルの製造に関する情報を、承認済みの機関にのみ送信する
7. 完成およびパーソナライズされた PIV クレデンシャルを、承認済みの発行元機関にのみ送信する
8. カードの製造、活性化、発行に関するセキュリティポリシーを、文書化、実施および維持管理する

活性化の時点において、発行元は、PIV クレデンシャルを活性化しようとしている個人が、当該 PIV を申請した本人であることを IDMS に対して 1 対 1 バイオメトリック検証を行うことで確認するものとする（SHALL）。確認後、発行元は当該クレデンシャルを活性化するものとする（SHALL）。

A.2.9 利用の中断、失効および廃棄

有効なカードについてだけでなく、紛失したカード、盗難にあったカードおよび期限切れカードについても、その状態を把握しておくことは重要である。発行されたすべてのカードを対象とするカードレジストリを確立し、維持管理しなければならない（SHALL）。

A.2.10 現行のPIVクレデンシャル保有者に対する再発行

現行の職員に対してアイデンティティクレデンシャルを発行または再発行する場合、発行元機関は次の事項を実行すること（SHALL）。

1. 当該個人の IDMS レコードがクレデンシャルの期限が切れていないことを示しているか確認する
2. 当該個人を 1 対 1 バイオメトリック照合により IDMS レコードに照らして確認する
3. 当該個人を IDMS レコード内のディジタル写真画像に照らして確認する
4. バイオメトリックを採取し直す
5. 新しいクレデンシャルを発行し、IDMS レコードを更新する
6. 採取し直したバイオメトリックと新しいクレデンシャルレコードに発行元機関がディジタル署名する（SHALL）

付録B—PIVの有効性確認、公認、および認定

B.1 PIVサービスプロバイダの認定

[HSPD-12]の定めにより、すべてのカードは、公式の認定プロセスによって信頼性が確立されたプロバイダによって発行される必要がある。NIST は財政の許す限り、PIV カード発行者が認定を得るために必要となる条件を詳細に規定する予定である。また、NIST は（これも財政の許す限り）それらの認定条件に照らして PIV カードの公式発行元機関を認定するプログラムを、政府全体を対象として制定する予定である。これらの作業が完了するまでの間、政府機関は、PIV カードの発行元を自己認定しなければならない（MUST）。

B.2 ITシステムのセキュリティ公認および認定

上で述べた PIV サービスプロバイダの認定制度を実現するため、また、OMB Circular A-130 付録 III の規定に適合するためには、PIV サービスプロバイダで使用する IT システムが NIST SP 800-37『連邦政府情報システムに対するセキュリティ公認と認定ガイド（Guide for the Security Certification and Accreditation of Federal Information Systems）』に従って認定される必要がある（MUST）。セキュリティ公認は、1 つの情報システムにおける管理、運用および技術的なセキュリティ管理策についての包括的な評価である。NIST SP 800-37 では、公認のための公式のフレームワークと、以下に説明する PIV モジュールについて検証を行い、承認を得るための具体的な要件を定めている。[SP800-37]

B.3 本規格に対するPIV構成要素の適合性

NIST では、実装が本規格に適合するかどうかを検証する PIV 検証プログラムの制定を計画している。次に示す事項は、NIST がこのようなプログラムを確立するまでの間は必須要件ではない。プログラムの詳細については、用意できしだいhttp://csrc.nist.gov/npivp/にて公開する予定である。

PIV システムが FIPS 201 に適合すると認められるのは、当該 PIV システムを構成する各要素（カード、リーダ、発行元ソフトウェア、登録データベース）がそれぞれ個別の有効性確認要件を満たしたあとである。個別の有効性確認要件はそれぞれ異なる規格に基づくものであり、単独でそれらすべての規格を対象に製品の有効性を確認することを認可された検査機関は存在しないため、PIV システムは複数の有効性確認施設において検査を受け、それぞれの規格に関する確認を実施しなければならない。各種の PIV 構成要素と、現時点で定められている有効性確認要件についての要約を表 B-1 に示す。

表 B-1. PIV システムの構成要素および有効性確認要件

PIV 構成要素	有効性確認要件
PIV ICC	ISO/IEC 7816、ISO/IEC 10373（Part 1 および 3） ISO/IEC 14443（Part 1 から 4）、ISO/IEC 10373（Part 6） 暗号モジュールーFIPS 140-2
PIV リーダ	PC/SC
カード発行および維持管理システム	暗号モジュールーFIPS 140-2

B.4 暗号技術の検査および認定（FIPS 140-2 およびアルゴリズム標準）

PIV システム内の暗号モジュールはすべて（カード上および発行元ソフトウェアとも）、FIPS 140-2 に照らして全体としてセキュリティ Level 2 以上の認定でなければならない（SHALL）。[FIPS140-2]

FIPS 140-2 の検査施設は、NIST の米国自主試験所認定プログラム（NVLAP：National Voluntary Laboratory Accreditation Program）により承認された暗号モジュール検査（CMT：Cryptographic Module Testing）機関である。PIV システム向け暗号モジュールの供給を希望するベンダーは、いずれかの認定試験所を選択して検査を実施できる。ベンダーからのすべての提出物に対してこれらの機関で実施される検査は、認定されたものであり、個々のベンダーモジュールに対して暗号モジュール認定プログラム（CMVP：Cryptographic Module Validation Program）から検証認定書が発行される。CMVP は、NIST およびカナダ政府の通信安全保障局（CSE：Communications Security Establishment）が共同で運営するプログラムである。CMVP および NVLAP 各プログラムの詳細と CMT 機関の一覧については、CMVP の Web サイトhttp://csrc.ncsl.nist.gov/cryptvalを参照のこと。

付録C—身元調査の詳細

以下では、NAC および NACI の詳細について説明する。

+ **NAC**:NAC はすべての NACI に含まれる。標準 NAC としては、セキュリティ／適合性調査指標（SII：Security/Suitability Investigations Index）、国防に関する利用許可および調査指標（DCII：Defense Clearance and Investigation Index）、FBI 名前検査（FBI Name Check）、および FBI 国家犯罪歴指紋検査（FBI National Criminal History Fingerprint Check）がある。
+ **NACI**:すべての新規採用連邦職員に対して要求される基本的かつ最低限の調査。NAC と、個人の経歴情報のうち特定の領域を対象とした過去 5 年間にわたる記録の書面による照会および探索により構成される（照会は現在および過去の雇用主、在籍した学校、信用照会先、地域の法執行当局に送付される）。対象となる領域は次のとおりである。
    - 雇用（5 年間の履歴）
    - 教育（5 年間の履歴および最高学歴が確認される）
    - 居住（3 年間の履歴）
    - 信用照会先
    - 法執行当局（5 年間の履歴）
    - NAC

付録D—PIVオブジェクト識別子および証明書拡張

D.1 PIVオブジェクト識別子

PIV オブジェクト識別子の詳細を表 D-1 の一覧に示す。

表 D-1. PIV オブジェクト識別子

ID	Object Identifier（オブジェクト識別子）	説明
PIV 電子内容タイプ		
id-PIV-CHUIDSecurityObject	2.16.840.1.101.3.6.1	関連付けられる内容は、認証鍵マップおよび非対称署名フィールドを除く CHUID の連結内容
id-PIV-biometricObject	2.16.840.1.101.3.6.2	関連付けられる内容は、連結された CBEFF_HEADER + STD_BIOMETRIC_RECORD
PIV 属性		
pivCardholder-Name	2.16.840.1.101.3.6.3	属性値は DirectoryString タイプ。PIV カード保有者の名前を示す
pivCardholder-DN	2.16.840.1.101.3.6.4	属性値は X.501 タイプ Name。PIV 証明書内で PIV カード保有者に関連付けられている DN を示す
pivSigner-DN	2.16.840.1.101.3.6.5	属性値は X.501 タイプ Name。バイオメトリックデータまたは CHUID に署名した主体の PKI 証明書に登場する主体者名を示す
pivFASC-N	2.16.840.1.101.3.6.6	pivFASC-N OID は、X.509 証明書の subjectAltName 拡張に含まれる otherName フィールドで名前タイプとして使用されるか、CMS 外部署名内の署名付き属性として使用される（MAY）。名前タイプとして使用される場合の構文は OCTET STRING。属性として使用される場合の属性値タイプは OCTET STRING。いずれの場合も、値は PIV カードの FASC-N を示す
PIV 拡張鍵使用		
id-PIV-content-signing	2.16.840.1.101.3.6.7	当該公開鍵を PIV CHUID および PIV バイオメトリックの署名検証に使用できる（MAY）ことを示す
id-PIV-cardAuth	2.16.840.1.101.3.6.8	当該公開鍵が PIV カード保有者でなく PIV カードの認証に使用されることを示す

D.2 PIV証明書拡張

PIV NACI indicator 拡張は、クレデンシャルの発行時点における対象の身元調査状況を示す。PIV NACI indicator 拡張は常に非重要であり、すべての PIV 認証用証明書に含まれなければならない（SHALL）。この拡張の値は次のように設定される。

+ クレデンシャルの発行時点において、(1)FBI 国家犯罪歴指紋検査（FBI National Criminal History Fingerprint Check）が問題なく完了しており、かつ(2)開始されたが完了していない NACI がある場合、値は TRUE である。
+ クレデンシャルの発行時点において、対象の NACI が完了しており、問題なく審査を通過している場合、値は FALSE である。

ただし、次のいずれかに該当する場合、PIV 認証用証明書はいっさい発行してはならない（MUST NOT）。

+ 完了したが問題の生じた NACI がある
+ FBI 国家犯罪歴指紋調査が完了していない
+ 開始されていない NACI がある

PIV NACI indicator 拡張は、id-piv-NACI オブジェクト識別子により識別される。この拡張の構文は、次に示す ASN.1 モジュールにより定義される。本文書末尾の変更告知に記載した重要事項を参照のこと。

```
PIV_Cert_Extensions { 2 16 840 1 101 3 6 10 1  }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

-- IMPORTS NONE --

id-piv-NACI  OBJECT IDENTIFIER  ::= { 2 16 840 1 101 3 6 9 1 }

NACI_indicator ::= BOOLEAN DEFAULT FALSE

END
```

付録E—物理アクセス制御メカニズム

政府のスマートカードに関する省庁間諮問委員会（Government Smart Card Interagency Advisory Board）の物理的セキュリティに関する省庁間作業部会（Physical Security Interagency Interoperability Working Group）による刊行物『*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* (PACS)』は、さまざまな保証プロファイルのための物理的アクセスに関するガイダンスである。表 E-1 に、PACS の保証レベルと、6.1 項で定義した PIV アイデンティティ認証の保証レベルとの対応関係を示す。

表 E-1. PACS 保証プロファイルと PIV の保証レベルの対応

PACS 保証プロファイル	PIV アイデンティティ認証の保証レベル
PACS Low（低）	SOME confidence（ある程度の信頼性）
PACS Medium（中）	SOME confidence（ある程度の信頼性）
PACS High（without PIN）（高、PIN なし）	SOME confidence（ある程度の信頼性）
PACS High（with PIN）（高、PIN あり）	VERY HIGH confidence（非常に高い信頼性）

付録F—用語集および略語集、表記規則

F.1 用語集

本規格中では次の用語を使用している。

アクセス制御／出入管理（Access Control）：以下の個別の要求を許可または拒否するプロセス。1）情報および関連する情報処理サービスの取得および使用。2）特定の物理的施設（連邦政府の建造物、軍事施設、国境通過出入口など）への立ち入り。

申請者（Applicant）：PIV カード／クレデンシャルを申請する個人。申請者になることができる（MAY）のは、連邦政府の被雇用者、連邦職員、委託業者のいずれかの身分に現在あるか、これらの身分におかれることが予期される者である。

アプリケーション（Application）：特定の要件群を満たすために実装されるハードウェア／ソフトウェア。この文脈におけるアプリケーションには、エンドユーザアイデンティティ検証または識別に関係する要求のサブセットを満たすために使用される何らかのシステムが組み込まれいて、エンドユーザアイデンティティを使用して当該エンドユーザによるシステムとの対話操作を促進できるようになっている。

承認済み（Approved）：FIPS によって承認された、または NIST によって推奨される（RECOMMENDED）ことを示す。（1）FIPS または NIST の推奨文書で規定されたか、（2）FIPS または NIST の推奨文書で採用された、アルゴリズムまたは技法。

アーキテクチャ（Architecture）：特定の問題を解決するためのフレームワークにおいて受け入れ可能なアプローチを表す高度に構造化された仕様。アーキテクチャは、選択された受け入れ可能なソリューションのすべての構成要素の記述を含む一方、個別の構成要素の詳細については関係する制約（費用、ローカルな環境、ユーザの受容性など）を満たせるように可変性を持たせている。

非対称鍵（Asymmetric Keys）：公開鍵とプライベート鍵という、対で使用される鍵。これらは、暗号化、復号、署名の生成、署名の検証といった相補的な処理の実行に使用される。

認証（Authentication）：真正性についての信用を確立するプロセス。本書における真正性は、個人のアイデンティティおよび PIV カードについての正当性に関するものである。

バイオメトリック（Biometric）：申請者の本人性を認識するため、または申請者の主張する本人性を検証するために使用される、測定可能な物理的特徴または個人の行動に関する特性。バイオメトリックの例としては顔写真画像、指紋、網膜スキャンなどがある。

バイオメトリック情報（Biometric Information）：バイオメトリックに関する、電子的に格納された情報。この情報は無加工または圧縮されたピクセルによって、もしくは何らかの特徴（パターンなど）に基づいて表現される。

バイオメトリックシステム（Biometric System）：次の機能を備えた自動化システム。

+ エンドユーザからバイオメトリックサンプルを採取
+ 採取したサンプルからバイオメトリックデータを抽出
+ 抽出したバイオメトリックデータと、1 つ以上の参照先に含まれるデータとを比較

+ 両者の合致の度合いを判定

+ 本人性の識別または検証に成功したかどうかを表示

採取（Capture）：エンドユーザからバイオメトリックサンプルを取得する方法。[INCITS/M1-040211]

カード保有者（Cardholder）：発行済み PIV カードを保有する個人。

証明書失効リスト（Certificate Revocation List）：認証機関によって作成され電子署名されたあとで失効した公開鍵証明書のリスト。[RFC 3280]

公認（Certification）：文言または主張の正しさを検証し、その正しさについての証明書を発行するプロセス。

認証局（Certification Authority）：公開鍵証明書の発行および失効を行う、信頼のおける機関。

認証要求者（Claimant）：認証プロトコルを使用して身元を証明する当事者。

比較（Comparison）：バイオメトリックと、事前に格納されている参照先とを比べるプロセス。「識別（Identification）」および「アイデンティティ検証（Identity Verification）」も参照。[INCITS/M1-040211]

構成要素（Component）：大きいシステムの部分をなす要素。PIV システムにおける構成要素としては、ID カード、PIV 発行元、PIV 登録機関、カードリーダ、アイデンティティ検証サポートなどがある。

適合性検査（Conformance Testing）：構成要素、製品、サービス、人、組織が備える特定の性質について FIPS に適合しているかどうかを検査するために、NIST が FIPS を策定、公布、サポートする責任の一環として確立するプロセス。

クレデンシャル（Credential）：個人の信用または権威の正当性を証明する証拠。本規格においては、権威をもってアイデンティティ（および、必要に応じてその他の属性）を個人に結び付ける、当該個人に関連付けられている PIV カードおよびデータ要素である。

暗号鍵（Cryptographic Key または Key）：暗号アルゴリズムと組み合わせて使用され、当該アルゴリズムにおける具体的な操作を決定するパラメータ。

連邦情報処理規格（FIPS：Federal Information Processing Standards）：情報技術ラボラトリ（ITL：Information Technology Laboratory）内で策定され、米国商務省の NIST によって公開された、連邦政府省庁および政府機関での採用および使用を目的とした標準規格。FIPS はそれぞれ、共通レベルの品質または一定レベルの相互運用性を実現するために情報技術に関する何らかのトピックを対象とする。

フレームワーク（Framework）：着目する 1 つのトピックに関する、解決すべき問題および達成すべき目標についての詳細な説明を含む構造化された記述。当該問題に対する受け入れ可能な解決策を策定するうえで取り組みが必要（MUST）なすべての事項に関し、注釈付きで概略を示したもの。受け入れ可能な解決策において満たす必要がある（MUST）制約事項についての説明および分析と、当該問題を解決するための受け入れ可能なアプローチに関する詳細仕様。

段階的セキュリティ（Graduated Security）：脅威、リスク、利用可能な技術、サポートサービス、時間、人的な考慮事項、および経済性に基づいて、いくつかの異なるレベル（たとえば低、中、高）で保護を提供するセキュリティシステム。

ハッシュベースのメッセージ認証コード（HMAC：Hash-Based Message Authentication Code）：暗号鍵をハッシュ関数と組み合わせて使用するメッセージ認証コード。

ハッシュ関数（Hash Function）：任意の長さのビット文字列を固定長のビット文字列に対応付ける関数。承認済みのハッシュ関数は次の性質を満たす。

1. **一方向（One-Way）**：あらかじめ指定された出力に対応する入力を計算によって求めるのが不可能であること。
2. **衝突への耐性（Collision Resistant）**：同じ出力に対応する 2 つの異なる入力を計算によって求めるのが不可能であること。

識別（Identification）：類似の人または項目で構成される集合全体の中で 1 人の個人または 1 つの項目の真の素性（すなわち身元、経歴）を発見するプロセス。

識別子（Identifier）：特定の個人の身元および関連属性を表現するために使用される固有のデータ。識別子の例として、名前、カード番号などがある。

アイデンティティ、または本人性（Identity）：特定の個人を一意に認識できるようにする身体的特徴および行動特性。

アイデンティティの結合（Identity Binding）：審査の対象となる主張されたアイデンティティを、発行元機関に従って（バイオメトリックにより）該当する個人に結び付けること。PIV クレデンシャルによって保持された、アイデンティティに関しての発行元による表明により表現される。

アイデンティティ管理システム（IDMS：Identity Management System）：アイデンティティを管理するためのシステム。アイデンティティの検証、有効性確認および発行プロセスを管理する 1 つ以上のシステムまたはアプリケーションにより構成される。

アイデンティティの立証（Identity Proofing）：身元を立証しようとする際に、PIV 登録機関に対して十分な情報（経歴、クレデンシャル、証拠書類など）を提示するプロセス。

アイデンティティの登録（Identity Registration）：特定個人のアイデンティティを PIV システムの知るところとし、当該アイデンティティに固有の識別子を割り当て、当該個人の適切な属性を採取してシステムに登録するプロセス。

アイデンティティの検証（Identity Verification）：アクセスを求めている人物のクレデンシャル（「持っているもの」、「知っていること」、「持っている特徴」）と、前もって立証され、PIV カードまたはシステムに格納され、主張されている身元情報に関連付けられているクレデンシャルとを比較することにより、主張されている身元が正しいかどうかを検証(肯定または否定)するプロセス。

識別可能な情報形式（IIF：Information in Identifiable Form）：ある情報が該当する個人について、その身元を直接または間接的な手段により合理的な程度に推測可能であるような、情報の表現形式。[E-Gov]

相互運用性（Interoperability）：本規格の趣旨における相互運用性とは、PIV 発行元にかかわらず、政府の任意の施設または情報システムが、PIV カード上のクレデンシャルを使用して当該カード保有者の本人性を検証できること。

発行元（Issuer）：申請者に対して PIV カードを発行する組織。普通、これは申請者の服務先の組織である。

JPEG:標準化された画像圧縮関数。元は合同写真画像専門家グループ(Joint Photographic Experts Group)によって策定された。

鍵（Key）:「暗号鍵（Cryptographic Key または Key）」を参照。

照合（Match または Matching）:バイオメトリック情報と事前に格納されているバイオメトリックデータとを比較し、類似性のレベルを評価するプロセス。

メッセージ認証コード（MAC：Message Authentication Code）:偶発的および意図的なデータ改ざんの両方を検出するために対称鍵を使用する、データの暗号チェックサム。

モデル（Model）:大きいシステムのうち 1 つの構成要素を、非常に詳細に記述または異なるスケールで表現したもの。最終的に作成される構成要素が実際の運用において備える特徴を予測する目的で、作成、運用および分析される場合がある。

カード外（Off-Card）:PIV カードの中に格納されないデータ、または PIV カードの集積回路チップ（ICC：Integrated Circuit Chip）によって実行されない計算処理を示す。

カード上（On-Card）:PIV カードの中に格納されるデータ、または PIV カードの集積回路チップ（ICC：Integrated Circuit Chip）によって実行される計算処理を示す。

1 対多（One-to-Many）:「識別（Identification）」の同義語。[INCITS/M1-040211]

オンライン証明書状態プロトコル（OCSP：Online Certificate Status Protocol）:公開鍵証明書の状態を知るのに使用されるオンラインプロトコル。[RFC 2560]

暗証番号（PIN：Personal Identification Number）:認証要求者が自身の身元を証明するために記憶し使用する秘密情報。PIN は数字のみで構成されるのが一般的である。

アイデンティティ検証カード（PIV Card：Personal Identity Verification Card）: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アイデンティティを、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、ディジタル表現された指紋など）が格納されているもの。

PIV 発行元（PIV Issuer）:身元証明カードの認可された作成者。FIPS 承認済みの空白の身元証明カードを調達し、要求されるアイデンティティ検証およびアクセス制御アプリケーションのために適切なソフトウェアおよびデータ要素を使用してそれらのカードを初期化し、認可された対象のアイデンティティクレデンシャルを使用してカードをパーソナライズし、さらに、保護と使用に関する適切な指示とともに、パーソナライズされたカードを当該の認可された対象に引き渡す。

PIV 登録機関（PIV Registrar）:申請者の身元を証明し、これを PIV 発行元に保証する主体。PIV 登録機関は、アイデンティティソース文書を検査しアイデンティティの立証を経ることで申請者の本人性を認め、かつ、クレデンシャルの発行前に、正しい身元調査が完了することを保証する。

PIV 保証人（PIV Sponsor）:省庁または政府機関に代わって申請者の PIV カードを要求することができる個人。

人口（Population）:対象アプリケーションのユーザ群。[INCITS/M1-040211]

公開鍵（Public key）：非対称鍵ペアのうちの公開の部分で、通常は署名の検証やデータの暗号化に使用される。

公開鍵基盤（PKI：Public Key Infrastructure）：PIV システムのサポートサービスの一種。ディジタル署名ベースのアイデンティティ検証を実行するため、また、アイデンティティカード内および検証システム内の取り扱いに注意を要する検証システムデータに関する通信および格納を保護するために必要とされる、暗号鍵を提供する。

推奨文書（Recommendation）：ITL の特別な刊行物の一種。共通のレベルの品質または一定レベルの相互運用性を実現するための、使用すべき技術に関する具体的な特性、または従うべき手順を規定する。

参照実装（Reference Implementation）：コンセプトの立証、実装の方式、技術の利用方法、および運用の実現可能性について実際に示すことを目的とした、FIPS の実装または NIST/ITL から入手できる推奨事項。

登録（Registration）：「アイデンティティの登録（Identity Registration）」を参照。

秘密鍵（Secret Key）：鍵を使用して暗号化されたデータを保護するために無許可での開示から保護されなければならない（MUST）暗号鍵。この文脈において使用されている「秘密（secret）」という語は、何らの機密性レベルを暗示するものではなく、開示または代替から当該の鍵を保護する必要性を示すものである。

規格（Standard）：1 つのトピックについて、当該規格に適合するために満たさなければならない(または達成しなければならない)（MUST）特性（通常は測定可能なもの）を指定する、公開された記述。

信頼性（Trustworthiness）：資格要件を判定および確認するための広範な調査、および、特定の作業と責務を行う適切性に関するセキュリティ上の決定。

有効性確認（Validation）：検討対象であるシステムが当該システムに関する仕様のすべての側面を満たしていることを実際に示すプロセス。[INCITS/M1-040211]

検証（Verification）：「アイデンティティの検証（Identity Verification）」を参照。

F.2 略語

本規格中では次の略語および頭字語を使用している。

ACL	Access Control List（アクセス制御リスト）
AES	Advanced Encryption Standard（次世代標準暗号化方式）
AIA	Authority Information Access（機関情報アクセス）
AIM	Association for Automatic Identification and Mobility（自動認識モビリティ協会）
ANSI	American National Standards Institute（米国国家規格協会）
CA	Certification Authority（認証局）
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）
CHUID	Cardholder Unique Identifier（カード所有者のユニークな識別子）
CIA	Cryptographic Information Application（暗号情報アプリケーション）
CMS	Cryptographic Message Syntax（暗号メッセージ構文）
CMT	Cryptographic Module Testing（暗号モジュール検査）
CMTC	Card Management System to the Card（カード管理システム対カード）
CMVP	Cryptographic Module Validation Program（暗号モジュール認定プログラム）
COTS	Commercial Off-the-Shelf（市販の既製品）
CRL	Certificate Revocation List（証明書失効リスト）
CSE	Communication Security Establishment（通信安全保障局）
CTC	Cardholder to Card（カード保有者対カード）
CTE	Cardholder to External System（カード保有者対外部システム）
DCII	Defense Clearance and Investigation Index（国防に関する利用許可および調査指標）
DN	Distinguished Name（識別名）
dpi	Dots Per Inch（インチあたりドット数）
DUNS	Data Universal Numbering System（データ汎用発番システム）
ECC	Elliptic Curve Cryptography（楕円曲線暗号）
ECDH	Elliptic Curve Diffie-Hellman（楕円曲線 Diffie-Hellman）
ECDSA	Elliptic Curve Digital Signature Algorithm（楕円曲線ディジタル署名アルゴリズム）
ERT	Emergency Response Team（緊急事態対応チーム）
FASC-N	Federal Agency Smart Credential Number（連邦機関スマートクレデンシャル番号）
FBCA	Federal Bridge Certificate Authority（連邦ブリッジ認証局）
FBI	Federal Bureau of Investigation（連邦捜査局）
FICC	Federal Identity Credentialing Committee（連邦個人認証委員会）
FIPS	Federal Information Processing Standards（連邦情報処理規格）
FIPS PUB	FIPS Publication（FIPS 刊行物）
FISMA	Federal Information Security Management Act（連邦情報セキュリティマネジメント法）
HMAC	Hash-Based Message Authentication Code（ハッシュベースのメッセージ認証コード）
HR	House of Representatives（米下院）
HSPD	Homeland Security Presidential Directive（国土安全保障に関する大統領令）
HTTP	Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）

I&A	Identification and Authentication（識別および認証）
IAB	Interagency Advisory Board（省庁間諮問委員会）
ICC	Integrated Circuit Chip（集積回路チップ）
ID	Identification（識別子）
IDMS	Identity Management System（アイデンティティ管理システム）
IEC	International Electrotechnical Commission（国際電気標準会議）
IETF	Internet Engineering Task Force（インターネット技術特別調査委員会）
IIF	Information in Identifiable Form（識別可能な情報形式）
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）
IT	Information Technology（情報技術）
ITL	Information Technology Laboratory（情報技術ラボラトリ）
JPEG	Joint Photographic Experts Group（合同写真画像専門家グループ）
LDAP	Lightweight Directory Access Protocol（軽量ディレクトリアクセスプロトコル）
MAC	Message Authentication Code（メッセージ認証コード）
MQV	Menezes-Qu-Vanstone（暗号化方式の一種）
NAC	National Agency Check（国家機関身元確認）
NACI	National Agency Check with Inquiries（照会を伴う国家機関身元確認）
NIST	National Institute of Standards and Technology（米国国立標準技術研究所）
NISTIR	National Institute of Standards and Technology Interagency Report（NIST 省庁間報告書）
NVLAP	National Voluntary Laboratory Accreditation Program（米国自主試験所認定プログラム）
OCSP	Online Certificate Status Protocol（オンライン証明書状態プロトコル）
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）
OPM	Office of Personnel Management（人事局）
PACS	Physical Access Control System（物理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／スマートカード間仕様）
PDF	Portable Data File（可搬データファイル）
PIA	Privacy Impact Assessment（プライバシ影響評価）
PIN	Personal Identification Number（暗証番号）
PIV	Personal Identity Verification（個人のアイデンティティの検証）
PKI	Public Key Infrastructure（公開鍵基盤）
pt	Point（ポイント）
RFC	Request for Comment（インターネット技術に関する IETF 発行文書）
RSA	Rivest Shamir Adleman（公開鍵暗号方式の一種）
SF	Standard Form（標準様式）
SHA	Secure Hash Algorithm（安全なハッシュアルゴリズム）
SII	Security/Suitability Investigations Index（セキュリティ／適合性調査指標）
SP	Special Publication（特別刊行物）

SSP REP Shared Service Provider Repository Service Requirement（共有サービスプロバイダのリポジトリサービス要件）

URI Uniform Resource Identifier（定形リソース識別子）

F.3 表記規則

本規格における「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 の記述に従って解釈される。

また、本規格文中の表記における字体の使用規則は次のとおりである。

+ *斜体*の用語（単語または連続した単語の列）は、ASN.1 データタイプを表す。たとえば、*SignedData* および *SignerInfo* はディジタル署名用に定義されたデータ型である。
+ 大文字の単語、または大文字の単語をアンダースコア記号で連結した文字列は、CBEFF 準拠のデータ構造を表す。たとえば、CBEFF_HEADER は CBEFF 構造に含まれるヘッダフィールドである。

付録G—参考文献

[ANSI322] ANSI INCITS 322 Information Technology, *Card Durability Test Methods*, ANSI, 2002.

[CBEFF] NISTIR 6529-A, Common Biometric Exchange Formats Framework (CBEFF), NIST, 2003.

[COMMON] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version 2.0, November 1, 2004.（入手先：http://www.cio.gov/ficc/documents/CommonPolicy.pdf）

[E-Gov] *E-Government Act of 2002*, U.S. Public Law 107-347, 2002.

[EO10450] Executive Order 10450, *Security Requirements for Government Employees*, April 17, 1953.（入手先：http://www.dss.mil/nf/adr/10450/eo10450T.htm）

[FIPS140-2] FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001.（入手先：http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf）

[G155-00] ASTM G155-00, *Standard Practice for Operating Xenon Arc Light Apparatus for Exposure of Non-metallic Materials*, Vol. 14.04, ASTM, July 2000.

[G90-98] ASTM G90-98, *Standard Practice for Performing Accelerated Outdoor Weathering of Non-metallic Materials Using Concentrated Natural Sunlight*, Vol. 14.04, ASTM, 2003.

[HSPD-12] HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

[INCITS/M1-040211] ANSI/INCITS M1-040211, *Biometric Profile—Interoperability and Data Interchange—Biometrics-Based Verification and Identification of Transportation Workers*, ANSI, April 2004.

[ISO10373] ISO/IEC 10373, *Identification Cards—Test Methods.Part 1—Standard for General Characteristic Test of Identification Cards*, ISO, 1998.Part 3—*Standard for Integrated Circuit Cards with Contacts and Related Interface Devices*, ISO, 2001.Part 6—*Standard for Proximity Card Support in Identification Cards*, ISO, 2001.

[ISO14443] ISO/IEC 14443-1:2000, *Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards*, ISO, 2000.

[ISO7810] ISO/IEC 7810:2003, *Identification Cards—Physical Characteristics*, ISO, 2003.

[ISO7816] ISO/IEC 7816, *Identification Cards—Integrated Circuits with Contacts*, Parts 1-6, ISO.

[NISTIR7123] NISTIR 7123, *Fingerprint Vendor Technology Evaluation 2003:Summary of Results and Analysis Report*, NIST, June 2004.

[OMB322] OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB, September 26, 2003.

[OMB404] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, OMB, December 2003.

[PACS] 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.

[PCSC] Personal Computer/Smart Card Workgroup Specifications.（入手先：http://www.pcscworkgroup.com）

[PRIVACY] *Privacy Act of 1974*, U.S. Public Law 93-579, 1974.

[PROF] *X.509 Certificate and CRL Profile for the Common Policy*, Version 1.1, July 8, 2004.（入手先：http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf）

[RFC2560] RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)*, Internet Engineering Task Force (IETF), June 1999.（入手先：http://www.ietf.org/rfc/rfc2560.txt）

[RFC3280] RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, April 2002.（入手先：http://www.ietf.org/rfc/rfc3280.txt）

[RFC3852] RFC 3852, *Cryptographic Message Syntax (CMS)*, IETF, July 2004.（入手先：http://www.ietf.org/rfc/rfc3852.txt）

[SP800-37] NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, NIST, May 2004.

[SP800-53] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, NIST, September 2004 (2PD).

[SP800-63] NIST Special Publication 800-63, *Electronic Authentication Guideline*, Appendix A, NIST, June 2004.

[SP800-73] NIST Special Publication 800-73, *Integrated Circuit Card for Personal Identity Verification*, NIST, February 2005.

[SP800-76] NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, NIST, February 2006.

[SP800-78] NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, March 2005.

[SSP REP] Shared Service Provider Repository Service Requirements, January 23, 2004.（入手先：http://www.cio.gov/ficc/documents/SSPrepositoryRqmts.pdf）

FIPS 201-1：連邦職員および委託業者のアイデンティティの検証
変更告知 1

U.S. Department of Commerce（米国商務省）
National Institute of Standards and Technology（米国国立標準技術研究所）
Gaithersburg, MD 20899

更新日：2006 年 6 月 23 日

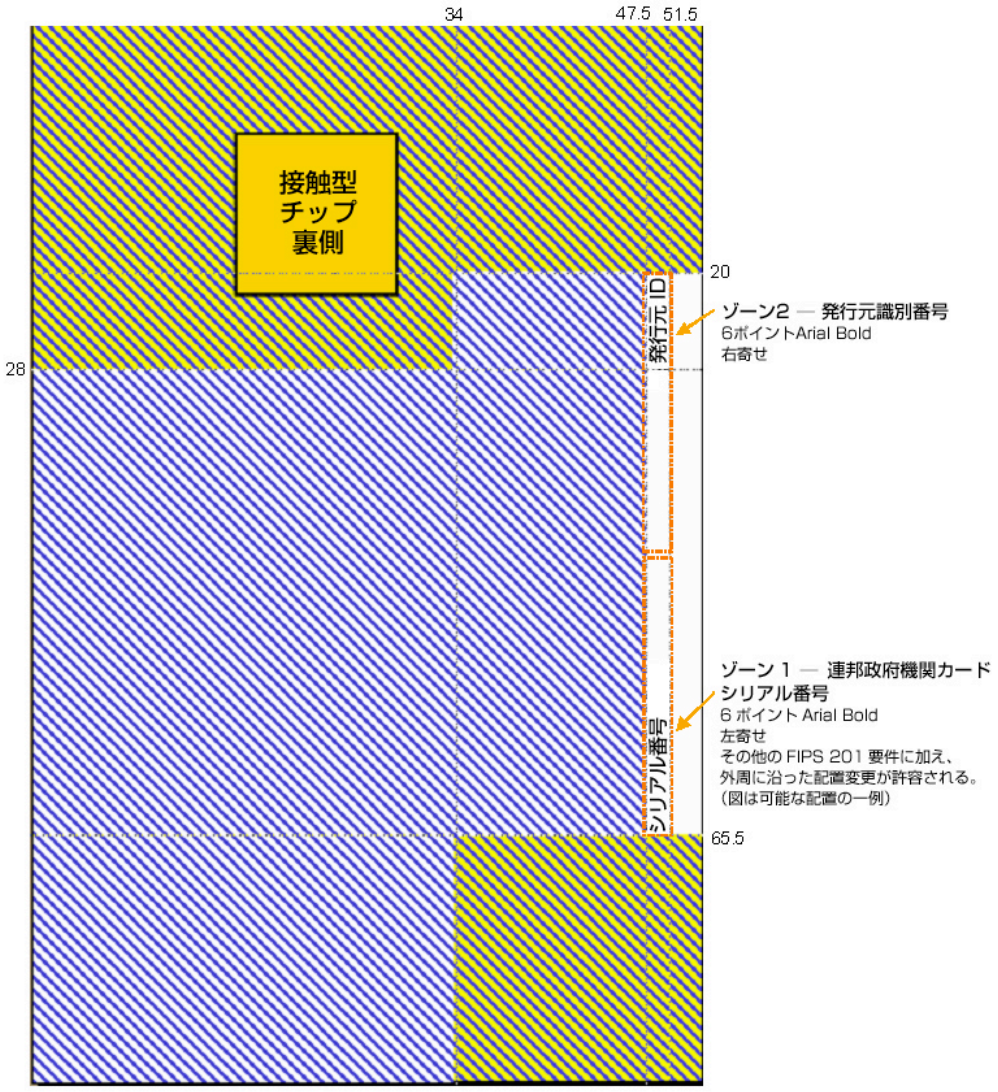
この変更告知に関する質問の送付先：piv_comments@nist.gov、または William MacGregor（william.macgregor@nist.gov、301-975-8721）

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、共通的な身元証明手段の標準を採用することを要求していた。FIPS 201-1『The Personal Identity Verification (PIV) of Federal Employees and Contractors（連邦職員および委託業者のアイデンティティの検証）』は、アイデンティティクレデンシャルに関する標準を確立するために策定された。本規格は、連邦職員および委託業者が共通的に使用する身元証明手段の標準について、アーキテクチャおよび技術的要件を定めるものである。総体的な目標は、連邦政府の管理下にある公的施設への物理的アクセスおよび政府情報システムへの電子的アクセスを求める個人について、当該個人が主張する身元を効率的に検証することにより、複数のアプリケーションにおいて適切なセキュリティ保証を実現することにある。

FIPS 201-1 は HSPD 12 の要件を満たすために策定され、商務長官の承認を受けたうえで 2006 年 3 月に発行された。この変更告知は、次に示すとおり、PIV カード裏側のグラフィックおよび NACI indicator の ASN.1 エンコーディングに関して変更を加えるものである。

日付	セクション、ページ	説明
2006/6/23	4.1.4.2、18 ページ	連邦政府機関カードシリアル番号の配置を PIV カード裏側の外周に沿った位置に変更することを認める。連邦政府機関カードシリアル番号の配置をより明確にするため、図 4-6 および図 4-8 の改訂版を下に示す。
2006/6/23	D.2、68 ページ	NACI indicator 拡張の ASN.1 モジュールから「DEFAULT FALSE」を削除し、次のとおりアンダースコア記号をダッシュに置き換える。 PIV-Cert-Extensions { 2 16 840 1 101 3 6 10 1 } DEFINITIONS EXPLICIT TAGS ::= BEGIN -- EXPORTS ALL -- -- IMPORTS NONE -- Id-piv-NACI OBJECT IDENTIFIER ::= { 2 16 840 1 101 3 6 9 1 } NACI-indicator ::= BOOLEAN END

周囲の寸法表示はミリ単位、左上隅からの長さ。
すべてのテキストは Arial フォントで印刷。
特記なき場合の推奨フォント—タグ：5 ポイント、太さ標準。データ：6 ポイント、太字。



任意データの領域。機関に特有のデータはこの領域に印刷する。任意使用データの配置に関する要件は、例を参照。

カード製造元により必要とされる可能性が大きい領域。任意使用のデータをこの領域に印刷してよいが、カードもしくはプリンタの製造元により指定される制約が適用される場合がある。

図 4-6. カード裏側－印刷に使用可能な領域および必須データ

周囲の寸法表示はミリ単位、左上隅からの長さ。
すべてのテキストは Arial フォントで印刷。
特記なき場合の推奨フォント―タグ：5 ポイント、太さ標準。データ：6 ポイント、太字。

図 4-8. カード裏側－任意使用データの配置－例 2