「米国における国民 ID と ID マネジメントを巡る動向」

和田恭＠JETRO/IPA NY

1．はじめに

社会全体の IT 化が進展する中、各種行政サービスの効率化や安全保障（テロ対策含む）の強化を進めるに当たり、国民に関する各種情報の照会・突合を可能とする個人識別手段が非常に重要な役割を果たすようになっている。このため、欧米を中心として統一的／行政分野別に国民ごとに番号を割り当てる個人識別番号（国民 ID）制度の導入が進められており、わが国においても、IT 戦略本部決定等[1]により国民 ID 制度の導入検討が進められているところである。

米国においても、連邦基準に沿った ID を国民や連邦職員に割り当てたり、IT による各種情報の管理効率化を進める動きがある。しかしながら、世界各国と同様、米国においても国民 ID の導入に関しては、プライバシー、個人情報保護、あるいは技術的な観点から様々な問題を抱えているのが現状である。また、その ID マネジメントに関しては、ID Theft などといわれる情報盗難・漏えいが発生しており、セキュリティの確保が大きな課題となっている。

今後の日本における IT 政策の進むべき方向およびそれらにかかる課題解決に向けた示唆を得るため、本稿では、国際動向にも触れつつ、米国における国民 ID と ID マネジメントを巡る動きとその問題点について報告する。

[1] 新たな情報通信技術戦略（平成 22 年 5 月 11 日 IT 戦略本部決定）において、2013 年までに国民 ID 制度の導入を行うことが決定されている。また、現在内閣官房国家戦略室で検討が進められている社会保障・税に関する共通番号のうち、中間報告における C 案が国民 ID に該当する。http://www.kantei.go.jp/jp/singi/it2/100511honbun.pdf http://www.npu.go.jp/policy/policy03/pdf/20100629/20100629_syakaihosyou_6_haihu.pdf 参照。

2. 国民 ID 及び ID マネジメントの国際動向

(1) 全体概要

国民に関する ID マネジメントについては、国際的にも取り組み方は様々である。下表に、主要国の国民 ID（に相当する ID）制度の特徴・情報連携の仕組み・個人情報保護システムの概要をまとめた。

【国際的な国民 ID 制度の導入状況[2]】

国名	ID の名称	情報連携の仕組み	ID の用途	個人情報保護法
米国	納税者番号（SSN）	社会保障庁（SSA）が管理し、内国歳入庁(IRS)や各州政府による利用が中心	納税手続きの電子処理化等	Privacy Act of 1974（適用対象は行政機関限定）
フランス	なし	行政分野ごとに異なる番号を利用	―	情報処理、ファイル及び自由に関する 1978 年 1 月 6 日の法律
ドイツ	なし	行政分野ごとに異なる番号を利用	―	連邦個人情報保護法(1977 年制定)
韓国	住民登録番号	行政自治部が管理し、各行政機関や金融機関が使用可能	納税、免許証申請、統計調査等	住民登録番号に関わる処罰法（2006 年制定）
デンマーク	国民登録番号（CPR）	国民登録局が管理し、各行政機関や金融機関等が使用可能	全電子行政サービスへのシングルサインオン等	個人情報の処理に関する法律（2000 年制定）
ベルギー	国民登録番号（RRN）	国民登録局が管理し、各行政機関が使用可能	社会保障に関する様々な申請の受付、関連情報提供等	個人データの処理に係る個人生活の保護に関する法律(1992 年制定)

以下、米国・韓国・デンマーク・ベルギーにおける国民 ID の制度各国における状況について概要を解説する[3]。

[2] 各種資料を基に著者作成

[3] このほか、カナダ（社会保険番号）、イギリス（国民保険番号）、スウェーデン(個人番号)、ノルウェー（住民登録番号）、フィンランド（国民識別番号）、オランダ（市民サービス番号）、エストニア（国民 ID 番号）、シンガポール（国民登録番

(2) 米国の概況

米国では国民 ID 制度は存在しないが、社会保障番号(Social Security Number：SSN)が実態的な国民 ID として用いられている。SSN の取得は任意であるが、米国民に加え、米国内で合法的に就労許可を得ている外国人も取得でき、納税・年金受給などの公共福祉サービス利用時に加え、銀行口座を開く際や与信を受ける時にも提示を要求されるため、事実上の国民識別番号となっている。

SSN に紐付けて管理される個人情報に関し、政府機関間の情報連携は限定的に行われており、同番号を発行する社会保障庁(SSA)と内国歳入庁(IRS)間で納税や個人所得に関する情報の共有が行われている[4]。加えて、一定の用途において州政府が SSN に紐付けられる情報を利用することも許可されている[5]。しかし、SSN を利用して普遍的に電子行政サービスを利用可能にする取り組みなどは存在しない。

＜米国の SSN カード[6]＞

個人情報保護に関する連邦法としては、Privacy Act of 1974 が存在し、連邦機関に対して本人の許可無く個人情報を第三者に譲渡することを禁止している[7]。1988 年の同法改正では、連邦機関によるコンピューター[8]使用に関する規定を追加している。ただし、同法の適用範囲は連邦機関に限られており、民間企業や法廷による個人情報取り扱いについて広範に規定した法律は存在しない[9]。

号)等、国民 ID 又はそれに相当する ID 制度を導入している国は多数存在する。
http://www.cipps.org/img/news/100701/ID%20number%20proposals.pdf 32 ページほか。

[4] http://www.law.cornell.edu/uscode/42/405(c)(2)(A).html

[5] http://www.law.cornell.edu/uscode/42/405(c)(2)(C)(i).html

[6] 著者に対して発行されたもの。右下の青い部分。

[7] http://www.usdoj.gov/opcl/privacyact1974.htm

[8] 原文では automated matching programs という名称を使っている

[9] 医療関係では、「医療保険の相互運用性と説明責任に関する法律(Health Insurance Portability and Accountability Act：HIPAA123)」等が存在する。ニューヨークだより 2010 年 9 月増刊号参照。

(3) 韓国における国民 ID 制度の概況

韓国においては、住民登録番号と呼ばれる国民 ID 制度が導入されている。これは、主に保安・国防を目的として 1960 年代に導入された番号制度を起源とするものである。原則として、韓国籍保持者でなおかつ韓国に在住する者全員に付番される(外国人には、個別に外国人登録番号が与えられる)。番号は 13 桁で構成され、ID カードには番号・氏名・顔写真・発給日時及び場所・指紋・住所変更履歴が記載されている。

＜韓国の国民 ID カード(左が表面、右が裏面)[10]＞

国民 ID のデータベース管理は、行政安全部によって行われている。情報連携の構築に関して、2001 年制定の電子政府法は、電子文書化推進やオンラインで行政サービス申請可能な環境を整えることを謳っており、韓国政府としては、最終目標として 70 種類に及ぶ行政機関発行の証明書が不要になることを目指している。既に入学・就職・多種多様な公的書類の申請・選挙投票者登録・統計調査時などの公用目的をはじめ、銀行口座の開設時や、民間企業が運営するオンラインサービスへの登録時にも使用され、韓国における国民 ID の使用用途は広い。

個人情報保護の体制としては、まず 1994 年制定の「公共機関における個人情報保護に関する法律」によって大枠が規定されている。また、国民 ID については 1962 年に制定された住民登録法が根拠法となっており、複数の改正を経て個人情報保護に関する条項が追加されていった[11]。また、韓国では近年電子商取引を通じた住民登録番号の盗用が問題になっており、この問題への対応も含めて、新たに「個人情報保護法」の制定に向けた動きがある。同法の枠組みの中には、個人情報保護のために大統領傘下に専門委員会を設立する計画もあるようだが、政治的な問題から、同法の成立はまだ実現して

[10] http://e-public.nttdata.co.jp/f/repo/592_a0812/a0812.aspx
[11] http://sonoda.e-jurist.net/korea/ronbun/kimjongcheol.htm

いない[12]。なお、上記の電子商取引における番号の盗用については、現行の対策として、i-Pin という仕組みが 2006 年に施行された。i-Pin とはいわば商用専用の住民登録番号であり、既存の住民登録番号を元にして希望者に発行されている。i-Pin の導入により、一般企業によって住民登録番号を収集されることがなくなるため、同番号の盗用被害が減少するなどの効果が期待されている。

(4) デンマークにおける国民 ID 制度の概況

デンマークにおいては、CPR 番号という識別番号が個人に振り当てられている。これは、地方行政団体が各々管理していた住民登録システムを、政府が 1968 年に全国的に統合したことが契機となっている。上記の韓国における国民 ID 制度と異なる点として、デンマークのシステムにおいては、一定期間同国に滞在する全ての人に登録が義務付けられていることが挙げられる。デンマークの国民 ID 番号は 10 桁で構成され、ID カードには生年月日・氏名・性別・住所が記載されている。ただし、個人用の ID カードは既に発行が停止されており、カード上に記載されている氏名や住所の更新も行われなくなったため、現在は ID カード自体を認証の手段として利用することはできない。1995 年 8 月には「personal IDentity card」という名称自体も廃止され、現在の国民 ID 制度はあくまでも番号ベースのみで運営されているようである[13]。

デンマークにおいては、国民登録局が国民 ID データベースの管理をしており、ほぼ全ての行政機関に アクセスが許可されている。それら公共機関の間で情報共有をすることで、国民に対する行政事務の円滑化・コスト削減を図っている。例えばデンマーク国内で引越しをした際に、地元の自治体で住所変更の手続きを行うと、変更した旨が国民 ID システムを利用する全ての行政機関に通知される。また、電子政府サービスにおいては一つの ID で全ての行政機関へのアクセスが可能になっている等、国民 ID を用いた認証の連携も行われている。また、一般企業にも専門端末を通して国民 ID データベースへの限定的なアクセスが許可されており、デンマークでは実生活のあらゆる場面で国民 ID が活用されていると言える[14]。

デンマークにおいては、2000 年制定の「個人情報の処理に関する法律（Act on Processing of Personal Data）によって個人情報保護に関する枠組みが確立されている。また、同法の成立と共に、データ保護庁（Danish Data Protection Agency）という独立機関も設立され[15]、行政機関・一般企業・個人が同法を遵守するための役割を果たしている。

[12] http://internet.watch.impress.co.jp/docs/column/security/20101007_398483.html
[13] http://www.cpr.dk/cpr/site.aspx?p=198&t=ForsideVisartikel&Articleid=4327
[14] http://www.fyidenmark.com/CPR.html
[15] http://www.datatilsynet.dk/english/

同法の特徴としては、米国や韓国等と異なり、適用範囲が公的機関と一般企業の両方に及んでいる点が挙げられる。

(5) ベルギーにおける国民 ID 制度の概況

ベルギーにおいては、RRN 番号という 12 桁の識別番号が個人に振り当てられている。これはベルギー国民全てに割り当てられるもので、番号と同時に eID カードと呼ばれる ID カードも給付される。15 歳以上の国民は、外出時に eID カードを常に携帯することが義務付けられている。ID カード上に記載されている情報としては、氏名・生年月日・顔写真・番号・国籍・性別がある。また写真からもわかるように IC チップも搭載されており、ここには上記情報が電子形式でも保存されている。なお、12 歳未満の子どもには、以下の写真とは異なるデザインのカードが給付される。

＜ベルギーの国民 ID カード[16]＞

ベルギーにおける国民 ID 制度の最大の特徴は、デンマーク同様、行政分野に加え、民間分野を含めた幅広い分野での活用がなされていることである。eID 保持者は、例えば、IC チップに保存されている電子署名を利用してオンラインバンキングを行ったり、一部の都市では専用のカードリーダーを経由して警察に犯罪の通報をすることができる[17]。また、子ども用 eID においては、両親が指定する数階層の電話番号が保存され、もしそれらの電話番号から応答がない場合には、チャイルド・プロテクション・ホットラインに自動的に転送される仕組みなども確立されている[18]。

個人情報保護の体制としては、1992 年制定の「個人データの処理に関わる、個人生活の保護に関する法律(Law on the Protection of Privacy Regarding the Processing of Personal Data)」によって大枠が規定されており、同法は 1999 年に改正を受けている。

[16] http://en.wikipedia.org/wiki/File:Eid.jpg 券面は見本（specimen）。
[17] http://www.guardian.co.uk/technology/2007/oct/04/guardianweeklytechnologysection.idcards
[18] 同上。

同法は、デンマークと同じく、行政機関と民間企業の両方に対して、個人情報保護に関する取り決めをまとめている。加えて、議会直属のプライバシー委員会が設置されており、デンマークのデータ保護庁と似たような役割を担っていると考えられる。その他にも、eID保持者は「Myfile」と呼ばれるサービスを利用し、どのような情報が登録局によって保持されているか調べることができる[19]等、市民による行政機関の監視の実現を目指した取り組みも見受けられる。

[19] 同上。

3. 米国における ID マネジメントの概要と課題

(1) 全体像

現在、米国では全ての国民が共通して所持する国民 ID というものは存在しない。従って、米国内で公的に個人のアイデンティティーを証明する必要がある場合、連邦政府発行の社会保障番号（Social Security Number: SSN）、州政府発行の運転免許証または身分証明証カード、州政府によって医師や不動産業者に与えられる免許証、そして連邦政府職員や政府コントラクターのみに発行される ID カード等が ID として用いられる。

これら公的機関による ID システムに加え、民間レベルでの ID マネジメントも存在する。公的機関によるマネジメントと異なる点としては、国民の大多数を普遍的にカバーするシステムを追求するというよりも、民間サービスにおける利便性を追求する上での汎用性や、汎用性実現のための認証インフラ構築に焦点が置かれていることであるといえる。

下表に、米国において公的な個人認証が必要な際に用いられる ID システムの概要をまとめた。

【米国における ID システムの概要】

名称	発行機関	発行対象者	主用途	従たる用途
SSN	連邦政府 (社会保障庁)	米国民及び外国人で合法的に労働許可を受けた者	社会保障給付、納税行為の整理・円滑化	左に加え、運転免許証・パスポート取得・銀行、クレジット口座開設時、雇用時における信用歴認証等様々な場面における個人識別[20]
運転免許証[21]	州政府[22] (車両管理庁)	外国人を含む全州民	運転免許保有の証明	左に加え、顔写真による確認が必要な、航空機を始め公共交通機関利用時の本人認証、年齢確認時等における個人識別
医師・不動産業者・弁護士等に与えられる免許	州政府 （各管轄機関）	専門職に従事するにあたり必要な技能を持つと証明された者	専門職免許保有の証明	—
PIV カード	各連邦政府機関	連邦政府職員及び政府業務請負業者職員	政府関連施設及び情報システムセキュリティの強化	—

[20] http://www.americanchronicle.com/articles/view/3911
[21] 運転免許証未所得者向けに発行される ID カードも同様。この場合、主用途が本人認証となる。
[22] ハワイ州とケンタッキー州においては、郡政府が管理する。

上表の中でも、SSN は、他の 3 つの公的機関発行 ID を取得する際に提示を求められることや、個人の信用歴や、連邦政府機関による個人調査時にも必要とされることなどから、事実上、国民 ID システムの基盤として位置づけられている。

ただし、SSN というシステム自体は、あくまでも個人名、SSN、そして各個人の生年月日という3つの情報に基づくシステムであり、写真などを含む視認による確認が可能な個人認証制度ではない。つまり、目前にいる人物が名乗っている名前が、本人自身であるという証明が必要な場合、通常、SSN の代わりとして、または SSN と併せて、州政府発行の運転免許証や写真付 ID カードが用いられる。これらは現在、全米 50 州が独自に発行しており、州ごとに運転免許証や ID カードのデザインや色柄は異なる。

しかしながら、運転免許証や ID カードについては、その発行に際し、顔写真・生年月日・氏名の掲載が義務付けられていること、またセキュリティ強化の為に複数の州がホログラムや生体認識技術など偽造を難しくする技術を導入しつつある[23]ことから、紙に名前と番号が印刷されているだけの SSN カードを補完する ID システムとして位置づけられている。このような状況を鑑みると、米国においては州政府発行の運転免許証や写真付 ID カードが、個人の証明をする上で最も一般的な国民 ID ともいえる。

以上のように、米国では、国民 ID の用途には SSN 及び運転免許証等が用いられており、統一的な国民 ID の策定及びそれを用いた国内各政府組織間での情報共有への取り組みは限定的であるが、インターネットを介して公的機関が個人の認証を行う際に、各連邦機関の間で統一された認証の仕組みを導入する目的で、2003 年に「E-Authentication」という取り組みが開始された。同取り組みについては、同年に行政管理予算局より発行されたガイドライン[24]において、「電子政府業務を行う上で、遠隔的に人間ユーザーが連邦機関の IT システムにアクセスする際の個人認証」を行うものであるとしており、各連邦機関に「認証プロセスの際に生じるリスクを検証し」、アクセスされる対象の機密性に対応した「4 つの ID 信頼性レベルを導きだす」ことを要求している。

これを実現するため、「E-Authentication の技術ガイドラインに基づいて、適切なテクノロジーを選択すること」もガイドライン中に規定されており、この流れを受けて、2009 年には「Open Identity for Open Government[25]」というイニシアチブが開始された。これは OpenID や Information Card といった民間主導の ID システム(後述)を用いて電子政府

[23] http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=15878
[24] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf
[25] http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV
http://www.readwriteweb.com/archives/openid_going_mainstream_us_gov_announces_pilot_pro.php

へのサインオンを可能にする為の、米国政府と複数ベンダー[26]間の取り組みであり、遅まきながらも上記ガイドラインに規定された枠組みの構築に向けた動きが出てきているようである。

将来的にこれらの取り組みが実現すれば、電子政府サービスの利用が市民にとって容易かつ便利になるだけでなく、民間分野も含めた複数のサービスで同じ ID が使われることで、それらサービス間の情報共有が深まり、個人にカスタマイズされたサービスも可能になると考えられる[27]。しかし、これらのイニシアチブは現在トライアル段階にあり、もし本格展開が可能としても、それが実現するまでには相当の時間を要するものと見られる。

(2) 国民向け ID システム

① 社会保障番号（連邦政府発行[28]）

- **歴史**

  社会保障番号（Social Security Number: SSN）は、社会保障プログラムの設立に伴い、社会保障の給付を円滑に行うことを目的として 1936 年に設置されたもので、現在の米国においては、雇用の際や社会保障給付金（Social Security benefit）の受け取りの際に必要な 9 桁の番号である。SSN の役割や利用される場面、取得できる資格などは、導入以降現在に至るまで、幾度かの変遷を経ている。

  役割については、1943 年、連邦政府機関が新規の ID システムを構築する場合には SSN をその基盤として採用する事が決定された。また、1961 年の内国歳入法（Internal Revenue Code Amendments）の改正により、納税時に社会保障番号を明記することが義務付けられ、翌 1962 年には SSN が正式な納税者番号として採用されるに至っている[29]。また、1970 年に成立した Bank Records and Foreign Transactions Act は、すべての銀行や信用組合（Credit Union）、およびその他の金融機関に対し、顧客の社会保障番号を取得することを義務付けた。その後 1974 年に発行された Privacy Act は、連邦政府および州政府機関に対し、国民に SSN の提示を求める際、SSN の提示が必須であるか、それとも任意でよいのかを明らかにするよう義務付けている。

---

[26] Yahoo!、Google、PayPal、Equifax、AOL、VeriSign、Acxiom、Citi、Provo、Wave Systems の 10 社と、Center for Information Technology、National Institutes of Health、Department of Health and Human Services の 3 政府機関に加え、それら政府機関の関連組織。
[27] http://www.readwriteweb.com/archives/openid_going_mainstream_us_gov_announces_pilot_pro.php
[28] http://www.socialsecurity.gov/history/pdf/2007historybooklet.pdf
http://www.socialsecurity.gov/history/ssn/ssnchron.html
[29] http://www.socialsecurity.gov/history/pdf/2007historybooklet.pdf

その後、1976 年税制改革法（Tax Reform Act of 1976）の成立に伴い、社会保障や公的支援の受け取りのみならず、運転免許証や車両登録の取得の際にも SSN が必要となった[30]。さらに 1998 年の「Identity Theft and Assumption Deterrence Act of 1998」では、名前、出生証明、自動車免許証、外国人登録カード番号、パスポート番号、などと並べて SSN も個人識別の方法の 1 つに定められ、これらの情報の不正使用は犯罪行為であり、処罰の対象となることが定められた[31]。

取得資格については、制度発足当時から 1986 年ごろまでは、14 歳前後までの子供は就労資格がないため SSN を取得できなかったが、現在では、国民は出生と同時に SSN を申請することが可能である[32]。なお、1972 年には合法的に米国に入国・滞在している外国人が社会保障番号を取得できるようになったが、1978 年には社会保障局が SSN 取得申込者に対して、申込者の国籍、年齢、本人確認の証明を求めるようになった。

- **SSN の問題点と解決に向けた取り組み**

SSN は、銀行口座残高の電話などでの問い合わせや、携帯電話やガス、電気の申し込み時の本人確認の際に使われることもある。このため、悪意ある第三者がある人の SSN を取得した場合、本人に成りすますなどの悪用が容易である。これに加え、SSN カードの偽造も問題の 1 つとなっていたため、2004 年に成立した Intelligence Reform and Terrorism Prevention Act の項目の一部で SSN カードの再発行回数の上限が定められると共に、カードのデザインを改めて偽造を防ぐことも決定された。

また、これまでに、不法労働者の取締りの一助として、SSN カードに生体認証を組み込という法案が議会に提出されているが、これについては議論も多い[33]。また、最近では、SSN を身分証明として使用することを制限するという法案も検討されている[34]。

② 運転免許証・ID カード（州政府発行）

米国では、連邦政府ではなく州政府によって、運転免許証又は免許未取得者を対象とした ID カードが発行されており、州ごとに運転免許証等の発行条件が異なる[35]。例えば、カリフォルニア州を例に取ると[36]、初めて運転免許証を取得する場合は、州

[30] また、同法により、SSN の不正使用と不正開示、漏洩が罰せられることも定められた。
[31] Identity Theft and Assumption Deterrence Act of 1998 (P.L. 105-318), http://www.ftc.gov/os/statutes/itada/itadact.htm
[32] http://www.socialsecurity.gov/history/ssn/ssnchron.html
[33] http://epic.org/privacy/biometrics/testimony_071802.html http://www.wired.com/politics/onlinerights/news/2007/05/biometric
[34] http://news.cnet.com/Congress-may-slap-restrictions-on-SSN-use/2100-7348_3-6071441.html?tag=nefd.top http://www.wired.com/politics/security/news/2003/01/57395
[35] http://www.chicago.us.emb-japan.go.jp/con_realID.htm
[36] http://www.dmv.ca.gov/dl/dl_info.htm#two500

内各地に設置された車両管理局（Department of Motor Vehicles: DMV）に行き、SSN や出生証明、合法滞在資格を証明する書類などを提出して免許証の発行を受ける。発行に際しては、写真撮影と親指の指紋採取も行われ、写真は免許証上に掲載されるが、指紋については、現状では免許証には組み込まれていない。なお、同州の場合、免許証の申し込み時に提出された SSN は、正規のものであるかの確認のため、SSA に照合される。

2001 年のテロ事件以降、免許証の発行条件が厳しくなったり、セキュリティ面を強化したライセンスを発行する州が出てきている[37]。また、連邦政府レベルでも運転免許証等の発給手続き及び記載事項等について基準を定め、厳格に運用しようとする動きがある（後述の Real ID 参照）。

例えばバージニア州の場合は、2009 年以降、プラスティックのカードにレーザで刻印を彫って偽造しにくくするなど、セキュリティ面を強化した運転免許証が発行されている。新しい運転免許証には 2 つのモノクロ写真が印刷され、そのうちの 1 つは透かしになっている[38]。インディアナ州は、2001 年のテロ事件の実行犯のうち、1 人を除く全員が米国に合法的に免許証を取得していたことを受け、免許証の発行前に申請者のバックグラウンドを調査すべく、これまでの即時発行方式を改めて、10 日後に郵送で届けるシステムを採用している[39]。このほか、カリフォルニア、コロラドなどの 13 州[40]でも、顔認証システムや指紋などの生体認証技術を導入し、運転免許証の偽造を難しくしている[41]。

③　専門職業免許（州政府発行）

医師・不動産業者や弁護士といった、一部専門職従事者に与えられる免許についても、州政府により発行されており、これら専門職免許の取得条件も州によって異なる。ただし、これらの免許証は、個人認証の際に使われる ID としての利便性は低く、例えば TSA のセキュリティチェックポイントを通過する際や、公的機関に対する個人証明としては、多くの州で使用が認められていないか、他の ID と合わせて提示されなければならない。その理由としては、特定職業のみに対する ID であるため SSN 程

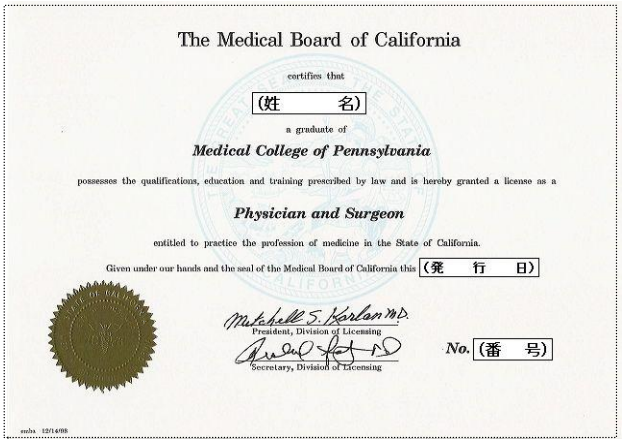
[37] http://www.dmv.state.va.us/webdoc/citizen/drivers/factsheet.asp
http://www.dmv.state.va.us/webdoc/general/news/dlci.asp
[38] なお、米国では、証明写真の撮影の際に笑顔で写ることも一般的であるが、同州は、免許証上の写真を撮影する際、笑顔で写ることを禁止している。これは、今後顔認証システムを構築していく上で、表情ができるだけ同じ方がシステムが上手く機能するためである。
http://www.washingtonpost.com/wp-dyn/content/article/2009/05/27/AR2009052703627.html
[39] https://myweb.in.gov/BMV/mybmvportal/LicensesAndIDCards/SecureID.aspx
http://www.fox59.com/news/wxin-drivers-license-changes-022610,0,4569235.story
[40] カリフォルニア州、コロラド州、コネティカット州、ジョージア州、ハワイ州、イリノイ州、オクラホマ州、ネブラスカ州、ニュージャージー州、南カロライナ州、テキサス州、ウェストバージニア州、ワシントン州
[41] http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=15878

のカバレッジがないこと、個人認証としての用途がもともと想定されておらず顔写真等も付されていないことが考えられる。

- **医療関係者免許の概要**

医療関係者が米国で免許を取得する際には、州政府の機関である医師会(Medical Board)に申請し米国医師国家試験(United States Medical Licensing Examination: USMLE、3 段階の試験で構成)を受けなければならない。申請に必要な条件や、申請時に要求される費用・書類、試験受験可能回数なども州ごとに多少の相違がある[42]。なお、ほとんどの州では 1-2 年の臨床経験(米国外のメディカルスクール出身者に対しては 2-3 年を要求する州も多い)が申請前に必要とされる。その他にも、いくつかの州では免許の取得申請時に指紋の提出が要求されるなど、詳細な身元調査が実施される。

各州の医師会ウェブサイトとも、医師の履歴情報に関する検索機能を搭載しており、医師が医療ミス・不祥事を起こしたり、他州で免許の停止・剥奪を受けた場合などには、これらの情報が開示される仕組みとなっている。なお、州間での医師に関する情報共有は限定的であるようで、複数の州において営業履歴がある医師について一度に履歴を表示するには、州立医師会連盟(Federation of State Medical Boards: FSMB)のウェブサイト上で検索する必要がある[43]。



The Medical Board of California

certifies that

(姓　　名)

a graduate of

Medical College of Pennsylvania

possesses the qualifications, education and training prescribed by law and is hereby granted a license as a

Physician and Surgeon

entitled to practice the profession of medicine in the State of California.

Given under our hands and the seal of the Medical Board of California this (発　行　日)

President, Division of Licensing

Secretary, Division of Licensing

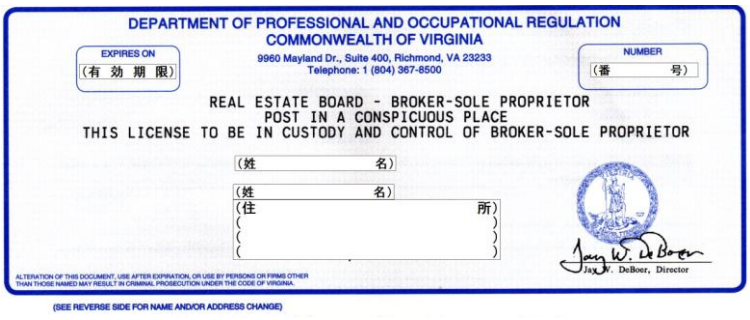
No. (番　号)

＜カリフォルニア州発行の医師免許＞

[42] http://fsmb.org/usmle_eliinitial.html
[43] サンプル: https://s1.fsmb.org/Docinfo/Forms/DocinfoSample.pdf

•不動産免許の概要

不動産免許の取得申請についての特徴は、州ごとに設定されたレギュレーションが大きく異なることである[44]。ただし、どの州も販売業者(salesperson)とブローカー(broker)の区分を設定しており、いずれの場合においても専門の学習課程を事前に修了することが要求される。加えて多くの州では、ブローカー免許を申請する前に販売業者としての経験を積んでいることも必要である。これらの条件を満たす者は不動産免許の試験を受けることができ、これに合格すると免許を付与される。なお、免許取得済みの者に対しても、定期的に学習課程を受けることを義務付ける州も複数存在する。ただし、これらの大まかな枠組みは多くの州で共通しているものの、必要な課程履修時間や、経験の年数といった細かい条件は、前述したように州ごとに大きな違いが見られる。

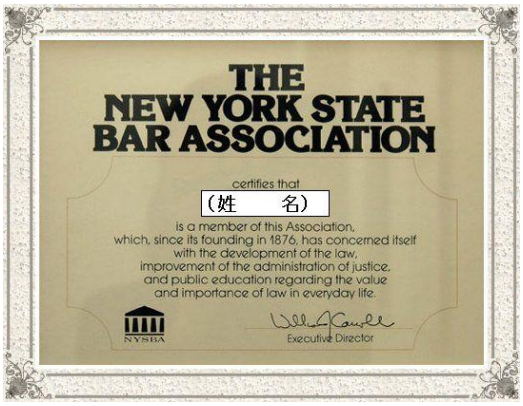

DEPARTMENT OF PROFESSIONAL AND OCCUPATIONAL REGULATION
COMMONWEALTH OF VIRGINIA
9960 Mayland Dr., Suite 400, Richmond, VA 23233
Telephone: 1 (804) 367-8500
EXPIRES ON
(有 効 期 限)
NUMBER
(番 号)
REAL ESTATE BOARD - BROKER-SOLE PROPRIETOR
POST IN A CONSPICUOUS PLACE
THIS LICENSE TO BE IN CUSTODY AND CONTROL OF BROKER-SOLE PROPRIETOR
(姓 名)
(姓 名)
(住 所)
Jay W. DeBoer, Director
ALTERATION OF THIS DOCUMENT, USE AFTER EXPIRATION, OR USE BY PERSONS OR FIRMS OTHER THAN THOSE NAMED MAY RESULT IN CRIMINAL PROSECUTION UNDER THE CODE OF VIRGINIA.
(SEE REVERSE SIDE FOR NAME AND/OR ADDRESS CHANGE)

＜バージニア州発行の不動産免許＞

•弁護士免許の概要

弁護士免許の取得についても、州によって条件が多少異なる。ほとんどの場合共通している点としては、(1)州政府または米国法曹協会(American Bar Association: ABA)認定の法学校を卒業していること、(2)Multistate Professional Responsibility Examination(MPRE)という、弁護士としてのプロフェッショナリズムを問う試験に合格すること、そして(3)司法試験に合格すること、の 3 項目が免許の交付を受ける上での前提となる[45]。例外として、いくつかの州[46]では、判事や弁護士の下で一定期間働いた経験があれば、司法試験を受けることができる。また、(2)についても、独自の類似試験を実施している州[47]や、法学校においてプロフェッショナリズムに関する課程で一定以上の成績を得ていれば、免除される州[48]もある。

[44] http://www.mortgagenewsdaily.com/real_estate_license/
[45] http://www.ncbex.org/fileadmin/mediafiles/downloads/Comp_Guide/CompGuide_2010.pdf
[46] カリフォルニア州、バーモント州、バージニア州、ワシントン州。
[47] メリーランド州、ウィスコンシン州、ワシントン州、プエルトリコ。
[48] コネチカット州、ニュージャージー州。



＜ニューヨーク州発行の弁護士免許＞

(3) 連邦政府職員向け ID システム

連邦政府職員やコントラクターの ID については、2004 年に発表された HSPD-12 に基づいて既に統一規格が策定されており、現在、各省庁レベルで、その規格に基づいた ID カード発行が進められている（詳細は後述）。

ID システムの具体的な例としては、DOD による、Common Access Card（CAC[49]）と呼ばれる ID カードの導入が挙げられる。2006 年よりに導入された、HSPD-12 基準に準拠したこのカードには IC チップが埋め込まれており、チップの中には、個人を特定するための生体認証情報（指紋情報）が含まれている。また、チップのメモリー容量は 128 キロバイト、マグネットストリップやバーコードも装備されており、RFID として無接触認証を行うこともできる[50]。なお CAC は、DOD 管轄施設にアクセスする場合や、DOD 管理下のコンピューターや Web サイトにアクセスする場合に必要となる。

(4) 民間による ID マネジメント[51]

民間による ID マネジメントにおいては、サービス利用分野間での汎用性の確保と、それを実現するための認証インフラ構築に重点が置かれている。そのため電子商取引やそれらを仲介する民間企業による ID マネジメントのイニシアチブとしては、多サイト間のシ

[49] http://www.cac.mil/
http://www.dtic.mil/whs/directives/corres/pdf/cio011601cac.pdf
[50] http://www.federalnewsradio.com/?sid=1734133&nid=35
なお、CAC には SSN が表示されていた時期もあるが、現在は表記されていない。また、2012 年にはマグネットストリップに埋め込まれている SSN の情報も取り除かれる予定である。
http://www.cac.mil/assets/pdfs/Flyer-SSN_FINAL.pdf
[51] 民間分野における個人認証技術についての詳細は、ニューヨークだより 2008 年 9 月号参照。

ングルサインオン連携と、多要素認証システムを導入し情報セキュリティの向上を狙うものと二つの動きが見られる。以下、これらの動きに関する概況を紹介する。

① シングルサインオン連携システムの展開状況

オンラインサービスの隆盛に伴い、覚えきれないほど多数の ID とパスワードを持つ一般ユーザーが増えてきた中で[52]、既存の認証システム同士に相互運用性を持たせようという取り組みも活発になっている。また、政府主導の「E-Authentication」といったイニシアチブが進展を見せない中、これら民間のサインオン連携システムを電子政府用途に試験的に導入するという試みもなされてきている[53]。

サインオン連携システムの普及を目的とした民間組織のうち、代表的なものには、Kantara Initiative、OpenID Foundation、Information Card Foundation があり、相互運用可能なサインオンシステムの推進という方向性では一致しているものの、その活動内容や具体的なシステムの構築方法といった面で、多少の相違が見られる。各組織の活動内容と、それらが国民 ID システム構築に向けて関わる可能性があるかについて、以下簡単に説明する。

＊Kantara Initiative

Kantara Initiative は非営利団体で、AOL、BT、Intel、NTT、Oracle、Sun Microsystems（当時）等の企業を理事会メンバーとしており、Liberty Alliance 等7つの団体を前身として 2009 年 6 月に設立された。ユーザー認証を必要とする一般企業・公的機関提供の電子サービスに対して、異サービス間の連携認証システムを構築するための研究開発を行っている[54]。また、同 Initiative は 2010 年 2 月 26 日に、「Open Identity for Open Government」イニシアチブによって、トラスト・フレームワークプロバイダー[55]として仮認定を受けている[56]。後述の OpenID や Information Card Foundation と違い、法人顧客向けサービスを展開する企業・団体による採用を主に念頭に置いているように見受けられる。

---

[52] http://www.thetechherald.com/article.php/201038/6172/Google-adds-two-factor-authentication-to-Apps
[53] http://www.readwriteweb.com/archives/openid_going_mainstream_us_gov_announces_pilot_pro.php
[54] http://kantarainitiative.org/wordpress/programs/assurance-certification/
[55] トラスト・フレームワークプロバイダーとは、認証プロセスにおいて ID 保持者（電子認証を受けるエンドユーザー）、ID 保持者に認証を与える認証局（ID プロバイダー）、そしてそれらの認証の正確性に頼る機関（Relying Party: RP。例: オンラインサービスを提供する企業や公的機関）の三者が存在する中で、ID プロバイダーと RP に対し、ID 発行・使用に関してお互いがどれだけ信用できる機関であるか、を判断する手段を提供する業者・団体。詳細は http://openidentityexchange.org/what-is-a-trust-framework 参照。
[56] http://kantarainitiative.org/wordpress/programs/assurance-certification/

∗OpenID Foundation

OpenID Foundation は、OpenID と呼ばれるシングルサインオン連携システムの普及を目指す非営利団体で、2007 年 6 月に設立された。参加企業には Google、Yahoo、Microsoft、IBM といった大手 IT 企業があり、主に個人ユーザー向けのサービスを展開する企業・団体を対称に活動を行っている。この種の ID 管理システムの中では最も普及しているとみられ、同団体の発表によると、2009 年末には OpenID 利用可能なアカウント・ID が全世界で 10 億個存在し、900 万件のウェブサイトが OpenID をサポートしていたという[57]。また、Kantara Initiative と同様、「Open Identity for Open Government」イニシアチブによって、トラスト・フレームワークプロバイダーとして仮認定を受けている[58]。同サービスの課題としては、一つの OpenID で複数サービスの認証に対応しているが故に、盗難の被害にあった際には、これら全てのサービス上で OpenID が悪用される危険性もあることが挙げられる[59]。

∗Information Card Foundation

Information Card Foundation は、Equifax、Microsoft、Oracle、PayPal、Novell、Google の 6 社を中心に、2008 年 6 月に設立された非営利団体で、上の 2 組織と同じく電子 ID インフラの構築を目的としている。同団体は I-Card と呼ばれる電子身分証明書・会員証に当たるカードの普及を目指しており、同カードをサポートするサイトにおいては、アイコンをクリックするだけであらかじめユーザーが I-Card に登録しておいた情報が送られ、認証に使われるようになっている。そのため、情報をウェブサイト上で入力する必要がなくなることから、フィッシング詐欺に遭う可能性が低くなるという利点があるとされている[60]他、エンドユーザー・ID 認証者・I-Card 対応ウェブサイトの間で瞬時にデータの同期化が行えるという強みもある。I-Card の採用はまだ一部にとどまっているが、AAA(旧称 American Automobile Association、日本でいう JAF のような団体)や、Student Advantage(学生向けのディスカウント商品紹介プログラム)といった組織が、自らのサービスに I-Card のサポートを加えたことが挙げられる[61]。なお、Information Card Foundation も、上記 2 組織と同じく、「Open IDentity for Open Government」イニシアチブによって、トラスト・フレームワークプロバイダーとして仮認定を受けている[62]。

---

[57] http://openid.net/2009/12/16/openid-2009-year-in-review/
[58] http://openid.net/2009/12/16/openid-2009-year-in-review/
[59] http://www.readwriteweb.com/archives/the_troubles_with_openid_20.php など。
一方、OpenID Foundation としてはセキュリティに対する万全の対策を訴えている。
[60] http://informationcard.net/quick-overview
[61] http://www.studentadvantage.com/discountcard/
[62] http://openid.net/2009/12/16/openid-2009-year-in-review/

② 多要素認証システムの展開状況

多要素認証システムとは、主にウェブサイト上で個人情報が送受信されると想定されるときに、一般的な認証プロセスで使われる ID・パスワードという組み合わせに加えてもう一つ(または複数の)本人しか知り得ない情報を入力させることで、情報セキュリティの改善を目指す仕組みである。

多要素認証システムの導入は、連邦金融機関調査委員会(Federal Financial Institutions Examination Council: FFIEC)が 2005 年に発表したガイドライン[63]によって、オンラインバンキングを提供する金融機関に対して要求されている。ただし、2007 年に Sestus 社と BearingPoint 社が発表した調査[64]によると、恒常的に同ガイドラインの要求を満たす多要素認証を行っている金融機関は、全体のわずか 4%に過ぎなかったという。

金融機関にとって、このようなシステムを導入するにあたっては、コスト面や、利用する上での煩雑さといったリスクもあり、業界全体が上記ガイドラインの導入に動いているというよりは、各社が独自の判断で取り組みをしているというのが現状である。また、同システムは、高リスクの取引におけるセキュリティの向上に必要とされているものの[65]、ガイドライン適用対象が今のところ金融機関にほぼ限定されているため、多要素認証システム技術標準の画定に向けた動きなどはまだ見られない。

以上のように、民間における ID マネジメントシステムは、未だ限定的な用途・サービスのみがサポートしている場合がほとんどであり、国民 ID マネジメントについて、これらのシステムがどのような役割を果たしていくのかに関しては、不透明な部分も多いと言える。

(5) 国民 ID 制度における課題

国民の ID マネジメントに際しては、ID 情報を含めた個人情報の保護が非常に重要となってくる。以下では、民間分野で運用されているクレジットカード情報を中心とした個人情報の盗難対策と保護の重要性と、個人情報にまつわる犯罪の発生状況、これらの解決に向けた取り組みの概要を紹介する。

オンライン・オンライン上での個人情報の盗難については、件数自体は増減を繰り返しているものの、盗難された情報の数は年々増加する傾向にある。個人情報の盗難に関す

[63] FFIEC、"Authentication in an Internet Banking Environment" http://www.ffiec.gov/pdf/authentication_guidance.pdf
[64] https://www.sestus.com/vt/docs/Trends_in_MFA_NonCompliance.pdf
[65] http://www.ffiec.gov/pdf/authentication_guidance.pdf

る情報提供や防止のためのコンサルティング業務を行う IDentity Theft Resource Center（ITRC）は毎年、米国における ID 盗難被害の発生数と、被害を受けた可能性のあるデータ数を公開しており、2005～2009 年の調査結果を見ると、盗難件数は 2006 年に前年から倍増し、その後 2008 年まで大きく増加を続けるものの、2009 年には減少し、2007 年レベルにまで下がってきている。一方で、被害に遭った情報の件数は増減を繰り返している。また、ITRC は被害に遭った情報の件数と 1 件当たりの平均被害額も推定しているが、これについては年によって増減が激しく、2009 年には盗難情報件数で 600%増、一件当たり被害額は半減との結果が出ている。なお、ITRC はこの数値について、「（あくまでも推定であり、）はっきりとした情報は不明である」としている[66]。

【個人情報の盗難と被害に遭った情報の件数（2005～2009 年[67]）】

	2005 年[68]	2006 年[69]	2007 年[70]	2008 年[71]	2009 年[72]
盗難件数	157	321	446	657	498
被害に遭った情報数（推定）	66,853,201	19,137,844	12,771,724	35,619,255	222,477,043
被害額／件[73]	N/A	87,303ドル	48,941ドル	58,135ドル	29,162ドル
被害額（推定）	N/A	2800 万ドル	2183 万ドル	3819 万ドル	1452 万ドル

具体的な、個人情報の盗難方法は、オンラインとオフラインの 2 つの種類に大分できる。まず、オフラインについては、①ゴミ箱から請求書やその他の個人情報の記入がある書類を拾う、②クレジットカード決済の際のスキミング、③金融機関や企業を装い、個人情報の提示を求める、④本人の承諾なしに請求書などの送付先を変更し、情報を盗む、⑤財布やハンドバックを盗んでクレジットカードの情報、税金情報を盗み出す、などが挙げられる。ただしこれらについては、個人が十分に留意することで被害に遭う可能性を最小限に抑えることができると考えられている[74]。

オンラインでは、フィッシングやハッキング、スパイウェアなどの利用などの方法で個人情報が盗み出される事例が多いが[75]、一般的なインターネット利用者が送受信する情報が暗号化されておらず、第三者により傍受される場合もある。特に電子メールの利用時には、ID などの個人情報を含む場合でも暗号化されずに送受信される場合が多く、これらの情報の盗難に遭い易いと言える[76]。

---

[66] http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2009_Data_Breaches.shtml
[67] http://www.idtheftcenter.org/artman2/publish/lib_survey/index.shtml
[68] http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20051231_1.pdf
[69] http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20061231.pdf
[70] http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20071231_1.pdf
[71] http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_2008_final.pdf
[72] http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20100106_1.pdf
[73] http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf
http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2009_20100520.pdf
[74] http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html
[75] http://www.ipa.go.jp/about/NYreport/200504.pdf
[76] http://joi.ito.com/privacyreport/Contents_Distilled/JapaneseSection/US_J_p73-123.pdf

特にクレジットカードに関する情報盗難の場合、場合、被害に遭った本人は、自分がカードを作成したのではないことを証明しなくてはならないため、被害を回復するのに時間がかかることがあり、与信が付与されなくなる、銀行借り入れ利率が引き上げられるといった二次的被害を被ることが報告されている[77]。

(6) 個人情報の保護に向けた政府・議会の取り組み

個人情報の保護に向けた政府の取り組みとしては、連邦政府によるアウトリーチ活動や、議会での個人情報保護強化に向けた法案の提出などが挙げられる[78]。連邦政府のアウトリーチ活動には、OnGuardOnline.gov や IDManagement.gov と言ったウェブサイトにて、関連情報が提供されている。また、議会でも、成立に至った件数は少ないながらも、個人情報を適切に保護するための各種法案が提出されている。

まず、連邦政府の取り組みの 1 つである OnGuardOnline.gov は、連邦取引委員会（Federal Trade Commission: FTC）を中心に、30 以上の政府機関・産業団体・NGO などが参加するホームページである[79]。同ページは、インターネットセキュリティに関する総合的な情報を提供することを目的としており、カバーされるトピック範囲は、コンピューター、ネットオークション、P2P などの利用時のセキュリティと 19 項目に渡っているが、このうちの 1 つに個人情報の保護も含まれている[80]。個人情報の保護に関するページでは、個人情報の盗難の危険性と、被害に遭った際にその被害を最小限にとどめるため、どのように対処するかといった情報が掲載されている。

また、ID Management.gov は、一般調達局（General Service Administration：GSA）が管理するウェブサイトで、連邦政府における ID 管理に関する情報が掲載されたものである。同ウェブサイトで扱われる内容には、連邦政府共通の ID 基準である HSPD-12 や連邦政府内で利用される ID や証明書（Credential）、およびアクセス管理の共通化などが含まれている。

一方、議会でも、SSN をはじめとする個人情報保護の重要性を認識しており、これまでに数々の法案を提出している。以下、今期（第 111 議会）議会に提出された、個人情報保護を目的とした各種法案を表にまとめた。これらの中には、前期、前々期でも提出されたものの、成立に至らず再提出された法案も多く含まれているが、現状でも多くは委員会に提出されたのみで、成立には至っていない。

---

[77] http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf, page 23
[78] http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html
http://www.idtheft.gov/
[79] 参加機関の例としては、DOJ、DHS、FCC、米国商事改善協会（Better Business Bureau：BBB）
[80] http://www.onguardonline.gov/topics/overview.aspx

【第 111 議会で提出された、個人情報保護・盗難に関する各種法案[81]】

法案名	提出者	提出日
IDentity Theft Notification Act of 2009 (H.R. 133[82])	Elton Gallegly 下院議員 （共和党、カリフォルニア州）	2009 年 1月 6 日
Identity Theft Prevention Act of 2009（H.R. 220[83]）	Ronald Paul 下院議員 (共和党、テキサス州)	2009 年 1月 6 日
IDentity Protection Act of 2009（H.R. 2417[84]）	Michael Arcuri 下院議員 （民主党、ニューヨーク州）	2009 年 5 月 14 日
Social Security Number Fraud and IDentity Theft Prevention Act（H.R. 2472[85]）	Mike Coffman 下院議員 （共和党、コロラド州）	2009 年 5 月 19 日
A bill to amend the Internal Revenue Code of 1986 to provide taxpayer notification of suspected identity theft（S. 1119[86]）	Blanche Lincoln 上院議員 （民主党、アーカンサス州）	2009 年 5 月 21 日
Photo Identification Security Act（H.R. 3174[87]）	Marsha Blackburn 下院議員 (共和党、テネシー州)	2009 年 7 月 10 日
Personal Data Privacy and Security Act of 2009 （S. 1490[88]）	Patrick Leahy 上院議員 （民主党、バーモント州）	2009 年 7 月 22 日
Social Security Number Privacy and IDentity Theft Prevention Act of 2009（H.R. 3306[89]）	John Tanner 下院議員 （民主党、テネシー州）	2009 年 7 月 23 日
Safeguarding Social Security Numbers Act of 2009（S. 1618[90]）	Charles Schumer 上院議員 （民主党、ニューヨーク州）	2009 年 8 月 6 日
Medicare Identity Theft Prevention Act of 2010（S. 3574[91]）	Sherrod Brown 上院議員 （民主党、オハイオ州）	2010 年 7 月 13 日
Social Security Number Protection Act of 2010 （S. 3789[92]）	Dianne Feinstein 上院議員 （民主党、カリフォルニア州）	2010 年 9 月 15 日

[81] http://www.govtrack.us/congress/subjects.xpd?type=crs&term=Computer+crimes+and+identity+theft
[82] http://www.govtrack.us/congress/bill.xpd?bill=h111-133
[83] http://www.govtrack.us/congress/bill.xpd?bill=h111-220
[84] http://www.govtrack.us/congress/bill.xpd?bill=h111-2417
[85] http://www.govtrack.us/congress/bill.xpd?bill=h111-2472
[86] http://www.govtrack.us/congress/bill.xpd?bill=s111-1119
[87] http://www.govtrack.us/congress/bill.xpd?bill=h111-3174
[88] http://www.govtrack.us/congress/bill.xpd?bill=s111-1490
[89] http://www.govtrack.us/congress/bill.xpd?bill=h111-3306
[90] http://www.govtrack.us/congress/bill.xpd?bill=s111-1618
[91] http://www.govtrack.us/congress/bill.xpd?bill=s111-3574
[92] http://www.govtrack.us/congress/bill.xpd?bill=s111-3789 2010 年 9 月 28 日上院通過。

4. Real ID を巡る動向

(1) Real ID の発行を巡る過去の議論の変遷

米国では、統一された ID が存在せず、特に ID カードの発給手続が州間で統一されていないことがテロ対策上の問題であるとして、2005 年より Real ID と呼ばれる国民 ID カードの導入が進められている。国際的に見ても、ドイツが生体認証 RFID を組み込んだ国民 ID の導入を進めている他、ベルギー、イタリア、フィンランド、エストニアなどの西欧諸国やマレーシア、シンガポールなどの国々が導入している[93]。

米国でも、1936 年に SSN 制度が実施されて以降数度に渡って国民 ID の導入が議論されてきたが、これまでのところ否定的な見方が多く、実際の導入には至っていない[94]。具体的には、SSN が施行された当初は、年金システムと連動した口座番号の開設などに SSN が使われる予定だったが、SSN が普及していくにつれ、SSN が利用される場面が増え、徐々に国民 ID 的要素が強くなっていった。しかし、社会保障局（Social Security Administration: SSA）内に設置された SSN タスクフォースは 1971 年、SSN を国民 ID として利用することを拒否するとの決議を下し、1973 年には、厚生・教育・社会福祉大臣諮問委員会も、「国民 ID は望ましくない」との見解を示した。更にカーター政権下の 1977 年にも、SSN の国民 ID 化は無いことが再度強調され、レーガン政権も 1981 年、国民 ID の作成に反対するとしている。

クリントン政権期には、1993 年、SSN に基づいた「健康・安全カード（Health Security Card）」を全国民に対して発行するとの計画を発表したが、プライバシー問題などを巡ってこの構想は多くの反対にあい、実現には至らなかった。また、1999 年には、1996 年に成立した、SSN 情報を運転免許証に記載するとの条項を含んだ『不法移民の改革及び移民の責任に関する 1996 年法律（Illegal Immigration Reform and Immigrant Responsibility Act of 1996）』が廃止されるに至っている[95]。

---

[93] ドイツ　http://beforeitsnews.com/story/11667/Germany_to_Issue_RFID-enabled_National_ID_Cards.html
西欧諸国　http://www.novosec.com/documents/eCommerce_ElectronicIDcard.pdf
マレーシアの国民 ID
http://www.malaysia.gov.my/EN/Relevant%20Topics/Security%20and%20Safety/Citizen/NationalIdentity/Pages/myNationalIdentity.aspx
シンガポール国民 ID　http://www.ica.gov.sg/services_centre_overview.aspx?pageid=247&secid=153

[94] http://epic.org/privacy/id-cards/#state
http://www.ncsl.org/Default.aspx?TabId=13581

[95] http://epic.org/privacy/id-cards/#state　http://www.ncsl.org/Default.aspx?TabId=13581

(2) Real ID Act の成立（2005 年）

このように、米国における国民 ID の導入はこれまで複数回に渡り拒否されてきたが、2001 年に発生したテロ事件をきっかけに、国民 ID にかかる議論が再燃した[96]。例えば、テロ実行犯 19 名のうち、18 名が（違法入手も含め）州発行の ID を入手していたため、米国内での移動が自由に行えたという事実を背景に[97]、9･11 コミッションは 2004 年に発表した報告書の中で、今後のテロ対策の1つとして、「しっかりとした ID 制度を確立すべきであり、出生証明や運転免許証の発行に際しては、連邦政府が設立した（統一された）基準を設け、導入するべきである」との提言を発表している[98]。また、9･11 コミッションの Thomas Keen 議長[99]は、「テロリストにとって、移動の自由を与える旅券や ID（travel document）を発行することは、武器を与えることと等しい」と発言し、米国内で統一された ID が必要である点を強調している[100]。

9･11 コミッション報告書を受け、ブッシュ前大統領は 2004 年 12 月、各州政府による運転免許証をはじめとした ID カード発行時の連邦基準を策定することなどを盛り込んだテロ対策法である National Intelligence Reform Act of 2004[101]を成立させた[102]。

一方、James Sensenbrenner 下院議員（共和党、ウィスコンシン州選出）が中心となって Real ID Act の策定を進めていた。しかし、同法は 2004 年に下院を通過したものの、その後の進展に行き詰りを見せていた。このため同議員は、同法を Real ID Act 2005 として、別の法案（Emergency Supplemental Appropriation for Defense, the Global War on Terror, and Tsunami Relief, 2005[103]）の一部に盛り込んで再提出した[104]。その法案の主要な内容は、軍の費用をテロや津波対策に充てることであり、テロや津波対策といった内容を全面に押し出していたため、上下院共に圧倒的多数で可決された[105]。

---

[96] http://www.dhs.gov/files/programs/gc_1200062053842.shtm
[97] http://www.washingtonpost.com/wp-dyn/content/article/2009/06/13/AR2009061302036.html
[98] http://www.ncsl.org/Default.aspx?TabId=13581
[99] Thomas Keen 議長は前ニュージャージ州知事。
[100] http://www.washingtonpost.com/wp-dyn/content/article/2009/06/13/AR2009061302036.html
このほか、Oracle の Larry Ellison 代表が、米国に合法的に居住、及び滞在している全ての人物の指紋と写真をデジタル化して組み込んだ国民 ID カードの発行案を支持し、これを実現させるための技術を提供すると政府に申し出ている。この案に対しては賛否両論が巻き起こり、公聴会も開催された。公聴会における反対案の主な主張は、国民 ID の作成は「市民の自由・権利に抵触する」（Newt Gingrich 前下院･議長）というものであった。
[101] http://thomas.loc.gov/cgi-bin/query/z?c108:S.2845: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ458.108.pdf
[102]ただし、DOT が免許の最低限の基準を設け、各州と協議しながら導入していくという箇所については、翌 2005 年に Tsunami Relief, 2005（後述）が成立したことに伴い削除され、連邦政府は、自ら作成した ID 発行基準を直接州政府に指導することとなった http://epic.org/privacy/id-cards/#state
[103] http://www.govtrack.us/congress/bill.xpd?bill=h109-1268
[104] http://www.ncsl.org/default.aspx?tabid=13579 http://www.govtrack.us/congress/bill.xpd?bill=h109-418 http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf
[105] 下院では 368 対 58、上院では満場一致で可決。

(3) Real ID の概要

REAL ID ACT of 2005 の主な内容は、連邦政府が運転免許証などの ID カード発行の基準を定め、その基準に則って州政府が ID カードを発行するというものである。ID カードの申請に必要な情報は、写真、生年月日、住所、SSN 、合法的滞在･居住許可の種類及び市民権や政治的亡命の経験の有無、などで、これらのデータは、連邦および各州政府間で互換性のあるフォーマットとして保存され、政府機関間で共有される。また、これに伴い、ID カードの申請時に提出する書類も統一化されることになる[106]。

また、各州に対しては、外国人による申請受理の際に、申請情報を移民局、SSA、DHS などが保有するデータと照合し、ビザの種類や居住の合法性を確認する事が義務付けられる他[107]、米国人の場合でも、出生証明が確認される場合もある。照合に際しては、SSN を照合する場合は、SSA 管轄のオンライン照合システムである Social Security On-Line Verification（SSOLV）データベースが、出生証明・米国市民である証明については、National Association of Public Health Statistics and Information System (NAPHSIS）局管轄の Electronic Verification of Vital Events （EVVE）システムが利用される[108]。

これらのほか、ID カードに記載すべき情報として、対象者の氏名、生年月日、性別、ID カードの識別番号（SSN ではない）、顔写真、主たる住所、発行日及び有効期限、署名等をコンピューター処理可能な形で記載することが求められている。

このように、Real ID Act の下では、各個人が提出する情報が正当なものであるかが厳密に確認されるため、合法的に米国内に居住する人物以外は、免許証等の ID カードを取得することができなくなる。また、州が発行したものであっても、Real ID Act の連邦基準に沿っていない ID カードは連邦レベルの身分証明として認められなくなるため、国土安全保障面が大いに強化される事になると考えられる。

(4) 導入を巡る問題点

REAL ID ACT of 2005 への反対意見は非常に根強いが、その大半は、運転免許証が事実上の国民 ID 証明書になってしまうという点に集中している[109]。これは、同法では、

---

[106] http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf
[107] http://www.examiner.com/x-9270-LA-Border-and-Immigration-Examiner~y2009m6d17-DHS-resurrects-Real-ID-law-in-new-version-PASS-ID
[108] http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf
http://statewidegovrecords.com/ssn.php?title=SSN%20Records&cmp=ossn&OVRAW=Real%20Id%2C%20Social%20Security%20online%20Verification&OVKEY=social%20security%20verification&OVMTC=advanced&OVADID=66863672011&OVKWID=121168221511&OVCAMPGID=281158511&OVADGRPID=6787956399&OVNDID=ND1 naphsis.org/NAPHSIS/files/ccLibraryFiles/Filename
[109] http://www.realnightmare.org/news/105/

運転免許証の携帯は表向きは任意となっているものの、携帯していない場合、疑惑をかけられたり、取り調べられの対象となる可能性があるため、事実上の国民 ID システムの構築を促していると見る団体も多い。

また、提出したデータが多数の機関で共有されるため、プライバシーの侵害が懸念されることや、強力なサイバーセキュリティが必要な点も主要な反対意見の 1 つである[110]。これに加え、連邦・州政府間で互換性のあるシステムを築く必要があるため、実施にかかるコストが莫大であることも問題である。例えば、当時アリゾナ州知事であった Janet Napolitano 国土安全保障長官は 2008 年、「(Real ID Act は)膨大な経費を投資するに値しない法案であり、代替案でも充分その機能を果たす」として、同州では Real ID を導入しないとする州法を可決している。2009 年時点で、Real ID の導入を禁止する州法施行又は決議を行っている州は 25 に上る[111]。また、全米知事会、全米州議会議員連盟(National Conference of State Legislatures)、全米交通管理教会(American Association of Motor Vehicle Administration)が 2006 年 9 月に共同発表した推定は、Real ID の導入に際し、5 年間で 110 億ドルかかるとしており、これは、議会が当初見積もった 1 億ドルの 100 倍以上とはるかに高額である[112]。

一方、DHS は 2007 年の同法に基づく ID カード発給基準の提案時、REAL ID 実施のコストを 10 年間で 231 億ドルとする分析結果を発表したものの[113]、2008 年 1 月に発表した最終規則発表時の評価 では導入コストを 99 億ドル、各州の負担 39 億ドル以下と見積もっている[114]。

当初、Real ID の導入期限は原則 2008 年 5 月 11 日とされていた。しかし、コスト、導入にかかる技術、DMV の現状、市民や人権擁護団体によるプライバシー侵害の懸念などの様々な要因を受け、Real ID の導入に踏み切る州は無く、導入期限は同年 12 月 31 日まで延期された。また、DHS が課した 18 のベンチマークをクリアした州に対しては、導入が 2010 年 1 月 1 日まで猶予されていたが、2009 年 12 月 18 日、全 56 のうち 46 の州と米国領から、同月 31 日までの導入は不可能であるとの報告を受けたため、DHS は Real ID 導入の期限を 2011 年 5 月 10 日に延期している[115]。

---

[110] 同上。
[111] http://epic.org/privacy/id-cards/#state
[112] 同上。
[113] このうち 100－140 億ドルは州が負担するコストになると見積もられている。
[114] http://epic.org/privacy/id-cards/#state http://www.ncsl.org/Default.aspx?TabId=13581
[115] 2010 年 4 月現在。http://www.ncsl.org/Default.aspx?TabId=13581
なお、州が導入期限までに Real ID の導入を行えない場合、その州の住民は、飛行機に搭乗の際や、連邦関係や原子力関係の建物に入館する時などに、その州発行の ID カードが、身分証明として使えないことになる。また、すでに発行された ID カードについても、2014 年 12 月又は 2017 年 12 月以降は Real ID 対応のもの以外は使えなくなる。

(5) オバマ政権の動向と現状[116]

このように、根強い反対にあい導入が先延ばしとなっている Real ID であるが、オバマ大統領は、もともと 2008 年の選挙戦時にも Real ID に反対した経歴があり、Real ID の導入に対して消極的である[117]。また、同大統領が、同じく Real ID に対して批判的なスタンスを取る Janet Napolitano 氏を DHS 長官に任命したことから、Real ID Act の先行きはますます不透明となっている[118]。このような中、2009 年 6 月に、Daniel Akaka 上院議員（民主党、ハワイ州選出）らが、Real ID Act の改定案である Pass ID Act[119]を議会に提出した[120]。

Pass ID Act では、Real ID Act よりも基準を緩和し、州への技術的及び経費の負担も軽減しているが、連邦基準に沿った ID カードのみを連邦レベルの身分証明証として認めるという基本概念は同様である。また、各州に対し、免許証などの申請者が提出した情報について、移民局、SSA、DHS などのデータと照合し、ビザの種類や合法的居住の確認を行うことも同様に義務付けている[121]。Real ID Act との相違点は、各州が管理するデータを交換するための互換性のあるシステムの構築が求められていない点、各州が申請者の出生証明の照合を行う必要がない点、申請者から提出された書面の保管が電子的に可能な点等である。これに加え、個人情報の盗難を防ぐためのシステムへの高額の投資も免除されている[122]。その一方で、プライバシー保護の取り組み強化に関する条項が盛り込まれた。

Pass ID Act に対しては、Real ID Act の成立に関わった人物からの批判が多く、例えば、Real ID Act を提出した Sensenbrenner 下院議員は、Pass ID の導入は、ID 管理を 2001 年当時に戻すのと同じことであると述べている[123]。このように、Real ID の導入を巡り米国内で意見が分かれる中、Real ID Act の遵守期限が迫ってきており、今後の動向が注目される。

---

[116] 政権発足前の政策は不透明（2008 年 12 月）。http://www.infoworld.com/d/security-central/obama-will-inherit-real-mess-real-id-528
[117] http://www.cnn.com/2009/POLITICS/04/22/real.ID.debate/
http://usgovinfo.about.com/b/2009/01/02/obama-may-let-real-id-act-just-fade-away.htm
[118] http://www.dhs.gov/xabout/structure/gc_1232568253959.shtm
http://www.cnn.com/2009/POLITICS/04/22/real.ID.debate/
[119] http://www.opencongress.org/bill/111-s1261/show
[120] http://www.washingtonpost.com/wp-dyn/content/article/2009/06/13/AR2009061302036.html
[121] http://www.examiner.com/x-9270-LA-Border-and-Immigration-Examiner~y2009m6d17-DHS-resurrects-Real-ID-law-in-new-version-PASS-ID
[122] http://www.examiner.com/x-9270-LA-Border-and-Immigration-Examiner~y2009m6d17-DHS-resurrects-Real-ID-law-in-new-version-PASS-ID
[123] http://sensenbrenner.house.gov/News/DocumentSingle.aspx?DocumentID=132634

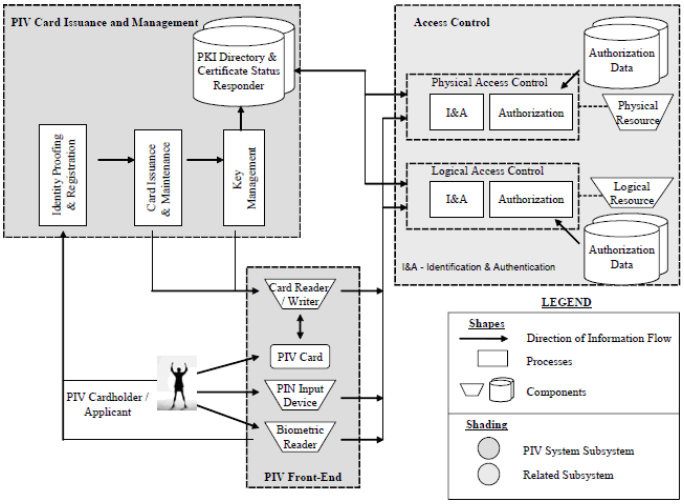
5. PIV カード（連邦政府職員向け ID カード）の導入を巡る動向

(1) PIV カードの概要

米国では、テロリズム、情報漏えい、個人情報の偽造といった脅威に対する政府関連施設および情報システムのセキュリティの強化を目的として、2004 年 8 月に発表された国土安全保障に関する大統領指令 Homeland Security Presidential Directives 12（HSPD-12）[124]に基づき、連邦政府職員および政府関係コントラクター向け個人識別情報検証（Personal Identity Verification: PIV）カードの発行を進めている。

HSPD-12 では、安全で信頼性の高い ID の要件として、①適切な基準に基づいて、各職員のアイデンティティが照合されている、②情報漏洩や偽造、テロリストによる悪用に強い、③電子認証を即時に行う事ができる、④公的に認定された信頼性の高いプロバイダーによって発行されている、という 4 つを定義しており、PIV カードはこれらを満たすものである必要がある。

【PIV カードを利用した認証の仕組み[125]】



同大統領指令では、PIV カードについて、接触・非接触の双方の通信方式に対応可能で、①生体認証データ（指紋）、②暗証番号、③非対称暗号鍵と証明書[126]、④カード保有者番号[127]、の 4 種類の情報を必須で盛り込むことを定めている。また、これらの情報に加

[124] http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html
[125] http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
[126] PIV Authentication data。
[127] Cardholder Unique Identifier（CHUID）。

え、省庁・機関ごとに、指紋以外の生体認証データなど、異なるデータを搭載することもできる。これらの情報は、カードに埋め込まれた IC チップに保存され、認証の際に、ネットワークを通じて照合が行われる。

(2) PIV カードに関する標準の策定動向[128]

HSPD-12 の一番の目的は、連邦省庁間で共通の ID カードを作成することにある。このため、同指令に基づき、商務省が PIV カードの発行を担当する各省庁が準拠すべき規格を策定することとされており、同省傘下の国立標準技術研究所（National Institute of Standard and Technology：NIST）は、連邦情報処理規格（Federal Information Processing Standard：FIPS ）201 の開発を行った。FIPS 201 は、2005 年 2 月に商務長官により承認、発行されている[129]。

① FIPS 201 の概要

FIPS 201[130]は、二部構成になっており、第一部(PIV-I)では、(1)PIV カード申請者の身元証明、(2)PIV カード発行と管理における必要規定、(3)PIV カード保有者のプライバシー保護、について規定している。第二部(PIV-II)では、PIV 運営システムの具体的な構成についての規格を記載しており、(1)PIV カード保有者が物理的に利用するインターフェース(PIV カード・カードリーダーと生体情報リーダー・PIN 番号入力機器)、(2)PIV カード発行・管理機構(身元証明・ID 登録・認証時に必要なデータベース等の体制)、(3)アクセス管理機構(PIV カード保持者が物理的または論理的なリソースにアクセスしようとする際、アクセス行為を管理するシステム)について規定している。以下に、PIV-I・PIV-II についての概要を記載する。

- **第一部（PIV-I）**

(1)身元証明をする際に順守されるべき条件に関しては、ID 発行の前に、最低でも FBI による犯罪歴調査(指紋調査)が必要であるとされている。その他にも、申請者は PIV カードが発行される前に、少なくとも一回は発行機関に出向くこと、行政管理予算局(Office of Management and Budget: OMB)規定による二種類以上の身元証明書類を提出すること、また身元証明・登録・カード発行が行われる際に、発行機関側でそれらのプロセスに関与する者が最低二人以上いなければならない、等を定めている。

(2)PIV カードの発行と管理に関しては、身元調査が正確かつ詳細に行われること、また ID の発行を受ける者が申請者と同一人物であることを確認すること、等が規定されている。

[128] http://www.nextgov.com/the_basics/tb_20080610_8037.php
[129] http://csrc.nist.gov/groups/SNS/PIV/index.html
[130] http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

(3)PIV カード保有者のプライバシー保護に関しては、各連邦機関による PIV システム運用の際、E-Government Act of 2002(電子政府法)、Privacy Act of 1974(プライバシー法)、そして OMB 覚書 M-03-22 によって規定された精神に則った運営がなされることを要求している。その他、もし PIV システムが HSPD-12 によって想定されていなかった用途で利用される場合、「セキュリティの向上、政府の効率性の向上、ID 不正使用の阻止、個人プライバシーの保護」の四原則を考慮するよう求めている。

- **第二部(PIV-Ⅱ)**

(1)PIV システムの物理的インターフェースに関しては、まず PIV カードが同システムで最も中心的となるコンポーネントであることや、同カードがクレジットカードサイズであること、そして最低でも一つの IC チップが搭載されていることを要求している。その他にも、認証方法として、「自身が持っているもの(“something you have”)」=PIV カードに格納された秘密鍵に加えて、生体情報リーダーを使用することによって「自身が誰であるかについて(”something you are”)」、PIN 番号を入力することによって「自身が知っていること(“something you know”)」の情報を利用可能となり、PIV 保持者に対してより高レベルの認証が行えることについても言及されている。

(2)PIV カード発行・管理のために利用される機構は以下のとおり規定されている。発行機構としては、カードの個人化(パーソナライゼーション)が行われるにあたって、物理的な側面(表面に印刷される写真、氏名等)と、論理的な側面(IC チップに記録される生体情報や電子署名等)が両方存在することを定めている。管理機構については、公開鍵の生成、電子証明書の発行と配給、そして電子証明書の状態に関する情報の管理と配布について言及されている。またこの管理機構は、公開鍵の生成と呼び出し、鍵の使用・更新・再発行・廃棄に至るまで、PIV カードライフサイクルの全過程において運用されることが規定されている。

(3)カード保持者がどのようなリソースにアクセスできるかを管理する機構については以下のとおり規定されている。リソースには、物理的なものと論理的なものがあるとして、前者は規制された施設(建物の玄関、部屋、駐車場の門等)、そして後者はネットワーク上に存在する仮想リソースや、ネットワーク設備(ワークステーション、コンピューター上のファイル・フォルダ、ソフトウェア等)であると定義している。アクセス管理機構は、各カード保持者に割り当てられているアクセス権利(privileges)を、カード保持者がアクセスしようとしているリソースに適用されている機密性と照会することによって、アクセス要請が受け入れられるか否かが決定される。

② NVLAP による認定制度の概要

FIPS 201 に沿って開発されたハードウェア及びソフトウェア製品・サービスは、実用化される前に、NIST 運営の NVLAP(National Voluntary Laboratory Accreditation Program)というプログラムによって認定された試験所でテストを受ける必要がある。このプログラムは、指定分野において、ベンダーによって開発された製品・サービスが NIST の規格に沿っているかどうかテストを行うだけの能力がある、と判断された

試験所に認定を与えるものである[131]。なお、厳密に言うと、FIPS 201 準拠製品・サービスのテストは、NVLAP で規定される複数テスト分野[132]のうち、CST LAP(Cryptographic and Security Testing Laboratory Accreditation Program)の管轄下で行われる。現在、民間の CST LAP 認定試験所は全米に 8 か所・カナダに 1 か所存在する[133]。

これらの認定試験所によって FIPS 201 準拠が認定された装置は、約 500 種類ある[134]。これら装置のうち代表的なカテゴリには、カードプリンター・IC チップリーダー・暗号用機器・電磁波シールド[135]・電子情報書き込み装置・顔写真撮影機・指紋採取機・PIV ミドルウェア・雛形作成機などがある[136]。

③ FIPS201 に基づく詳細規格

また、NIST は、FIPS 201 で定められた規格の詳細を定める文書として、①『個人認証におけるインターフェース（Interfaces for Personal IDentity Verification：NIST Special Publication 800-73）』、②『個人認証における生体認証データのスペック（Biometric Data Specification for Personal IDentity Verification：NIST Special Publication 800-76）』、③『個人認証における暗号アルゴリズムと暗号化キーのサイズ（Cryptographic Algorithms and Key Sizes for Personal IDentity Verification：NIST Special Publication 800-78）』、の 3 つの文書を発表している[137]。なお、インターフェースに関する文書に関してはその後も継続的に見直しが行われており、最新の第 3 版が 2010 年 4 月に発表されている。

【NIST による 3 つの FIPS 文書の概要[138]】

文書名	発行時期（最新版発表時期）	概要
個人認証におけるインターフェース	2005 年 4 月（2010 年 3 月）	PIV カードに組み込むインターフェースとデータの要素を特定。全 4 パートで構成。
個人認証における生体認証データのスペック	2007 年 1 月	PIV システムにおける、生体データの技術習得方法とデータフォーマットの要件を特定。
個人認証における暗号アルゴリズムと暗号化キーのサイズ	2007 年 1 月	PIV システムで導入、利用するべき暗号化アルゴリズムと暗号化キーのサイズを特定。

[131] http://www.nist.gov/pml/nvlap/about-nvlap.cfm
[132] http://ts.nist.gov/standards/accreditation/fields.cfm
[133] http://crsc.nist.gov/groups/SNS/PIV/nPIVp/testing_facilities.html
[134] http://fips201ep.cio.gov/apl.php
[135] “Electromagnetically opaque sleeve”. IC チップに保存されている情報への許可無きアクセスを防止する
[136] なお、製造者による保守期間の終了、FIPS 201 の改正により非準拠となった、または NIST による同規格内条項の解釈が変わった等の理由で承認取り消しを受けた製品も約 50 程度ある。http://fips201ep.cio.gov/rpl.php
[137] http://csrc.nist.gov/groups/SNS/PIV/index.html
[138] http://csrc.nist.gov/publications/PubsSPs.html

(3) 導入を巡る議論

HSPD-12（及び FIPS201）の要件に沿った連邦職員用 ID の作成に関しては、Real ID の場合と異なり、特に目立った議論は起こっておらず[139]、各省庁・機関における導入管理を担当する行政予算管理局（Office of Management and Budget：OMB）が定めるデッドラインに沿って作業が進められてきた[140]。

- デッドライン 1：2007 年 10 月 27 日までに、勤務歴が 15 年以下の政府職員、およびコントラクター企業全員の素性調査を行うと共に、これらの連邦職員や提携先企業社員に対し、生体認証データを含む PIV カードを発行する。
- デッドライン 2：2008 年 10 月 27 日、連邦政府職員全員に対する素性調査、および PIV カードの発行を完了させる。

しかし、技術的な問題[141]により、各省庁・機関における導入が困難になり、OMB は 1 度目のデッドラインの 4 日前に当たる 2007 年 10 月 23 日、PIV カードの一斉導入が不可能であることを認め、各省庁・機関に対し、定期的に進捗情報を公開することを条件に、独自のスケジュールで PIV を導入していくことを許可した。これにより、PIV カードの一斉導入は断念されることとなった[142]。

その後、各省庁は独自に PIV カードの導入を進めてきているが、ホワイトハウスが発表した最新の PIV カード導入報告[143]によると、2010 年 6 月 30 日の時点で、連邦政府職員の 70.1%に当たる 327 万 6,922 人と、契約企業社員の 60.4%に当たる 75 万 1,193 人に対し、既に PIV カードが発行されているとのことであった。

---

[139] 現状で見当たる唯一の議論は、2007 年 8 月、NASA のジェット推進研究所（Jet Propulsion Laboratory：JPL）の科学者および技師 28 名が、「HSPD-12 に則って NASA が行う、PIV カード作成・発行のための職員の素性調査は、職員のプライバシー侵害にあたる」として、連邦政府、および JPL を運営するカリフォルニア工科大学を相手取った訴訟を起こしたことのみである。なお、同件は最高裁にまで持ち込まれ、2010 年 10 月 5 日に口頭弁論がなされているが、判決には至っていない。http://hspd12jpl.org/lawsuit.html 参照。

[140] http://www.whitehouse.gov/omb/memoranda/fy2008/m08-01.pdf

[141] 具体的には、新しく作成された ID カードが GSA の検査を通らなかった場合、カードを新しく作成しなければならなかったことや、新しいカードと既存のアクセスコントロールシステムの統合が容易でなかったことが挙げられる。http://www.nextgov.com/the_basics/tb_20080610_8037.php 参照。

[142] http://www.whitehouse.gov/omb/memoranda/fy2008/m08-01.pdf

[143] http://www.whitehouse.gov/sites/default/files/page/files/HSPD-12_StatusReportDetails-Q3FY2010.pdf

本レポートは、注記した参考資料等を利用して作成しているものであり、本レポートの内容に関しては、その有用性、正確性、知的財産権の不侵害等の一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本レポートの読者が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。

なお、このレポートに対するご質問、ご意見、ご要望がありましたら、takashi_wada@jetro.go.jp までお願いします。