第１章　アメリカ・カナダの事例

図表目次

第１節　電子政府・電子自治体の情報ネットワーク基盤の現状

１　公共団体が保有する個人情報を有する主要データベースの共同利用

米国、カナダともに、日本で言うところの住民基本台帳のような全国規模で個人情報を一元管理するデータベースは存在しておらず、基本的には各地方団体[1]が独自のデータベースを独自に運営・管理している。このため、例えば米国では、運転免許書や医師免許といった各種免許が州ごとに発行されており、これらに関する規定や発行基準を州が独自に定めているほか、これら免許発行を通じて得られた情報については、各州それぞれが構築するデータベースによって管理が行われている。州政府間での個人情報の情報共有の必要性は低く、むしろ連邦政府と州政府との情報共有が重視されている。同様にカナダでも、全国規模での個人情報交換は行われていない。

このような米国・カナダにおける国と地方団体との情報ネットワーク基盤の仕組みを踏まえた上で、両国の地方団体が個別に実施している個人情報共有の取り組み例を以下に示す。

（１）国と地方団体間の情報共有

ア．米国

米国における連邦政府と地方団体間での情報共有は、主に公安目的のものが多い。従って、ここで共有される情報は、犯罪者や仮釈放中の者、テロリスト情報などが中心となる。住民基本台帳のような一般市民の個人情報を公共団体間で共有する例としては交通安全目的での運転免許証情報などがある。また、行政手続簡素化目的で納税者情報を連邦政府（内国歳入庁）と州政府が共有し、重複作業を回避する試みが実施されている。

以下では、

・連邦政府・地方団体間の公安情報共有システム
・連邦政府間、連邦政府・地方団体間のテロリスト情報共有
・連邦捜査局による捜査用データベース
・内国歳入庁・州政府間の納税者情報共有

の４つについて簡単に紹介している。

（ア）連邦政府／地方団体との公安情報共有システム

全国法執行機関通信システム（NLETS：The National Law Enforcement Telecommunication System）は、1966 年５月にアリゾナ州フェニックスの高速警備隊本部にて『LETS（The Law Enforcement Teletype System）』として始まった米国でも長い歴史を持つ全国規模の公安情報共有システムである。従来は、警察官が州外の自動車や運転免許証を調査することを目的としていたが、現在はこれら公安目的以外にも、矯正中の受刑者（仮釈放、執行猶予）や性犯罪者、行方不明児童の情報も共有する。同システムは現在、米国・カナダの連邦政府、並びに全州のシステムに相

[1] 以下、州を含めて地方団体と記述する。

互接続されており、毎月 4,000 件のデータ交換を３万箇所の施設で 50 万機の端末を介して行われている。

一方で、NLETS システムは、書面での契約あるいは覚書に基づいたシステム同士の接続であったため、その規模が拡大するに伴いその使い難さに対する不満が募っていた。例えば、交通警備中の警官が運転免許データを取得したい場合、必要以上の情報が小さな端末機に伝送されてしまうという事態が起きていた。このようなシステム面の問題を改善したのが、XML データを使用する GJXDM システム（Global Justice XML Data Model）の『全国情報交換モデル（NIEM：National Information Exchange Model）』である。同モデルは元来、連邦司法省（DOJ：Department of Justice）が省内の部局間（Bureau of Justice Assistance、Office of Justice Programs）を接続するために採用したシステムであるが、その後国土安全保障省（DHS：Department of Homeland Security）にも採用され、既存は NLETS のシステムとして採用されている。

NIEM は、既存のシステムを使用したまま XML フォーマットでのデータ交換を実現するため、既存のシステムをそのまま利用できるという点からのコスト削減効果も報告されている。例えば、アラスカ州政府公安局（Department of Public Safety）では、2004 年度のみで 2 万ドル、ミネソタ州政府公安局でも過去３年間で 1,000 万ドルのコスト削減効果が確認されている[2]。

（イ）連邦政府間／連邦政府と地方団体間のテロリスト情報共有

2004 年８月 27 日、ブッシュ大統領は大統領指令『米国民保護を目的としたテロリスト情報共有強化大統領指令（Executive Order Strengthening the Sharing of Terrorism Information to Protect Americans）』[3]を発行した。この大統領指令は、国土安全保障の観点から連邦省庁間での個人情報を含めた情報共有を向上させることを目的としたものである。従って、例えば健康保険や納税状況といった個人情報の共有という趣旨ではなく、むしろテロ活動の発見・防止とテロ活動による混乱の抑制を最優先としたテロリスト情報の共有が重視されている。また、この大統領指令では、

・連邦省庁間でのテロリスト情報交換
・省庁と州・地方自治体間でのテロリスト情報交換
・これらテロリスト情報を収集するための制度の保護

が最優先事項として掲げられている。

[2] GOVERNMENT ENTERPRISE 紙、2005 年６月２日。
http://www.governmententerprise.com/showArticle.jhtml?articleID=163700166
[3] 『米国民保護を目的としたテロリスト情報共有強化大統領指令（Executive Order Strengthening the Sharing of Terrorism Information to Protect Americans）』：
http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html

一方で、大統領指令が発令された約２ヵ月後の 2004 年 11 月９日、個人情報を国土安全保障目的で共有することに関する討論会が技術政策団体や市民擁護団体により開催されるなど、その情報共有の度合いに対する懸念も高まっている。例えば、人権擁護団体の米国市民自由団体（American Civil Liberties Union）は、「『個人情報の共有』により権力が乱用される可能性が高い」と批判を展開しており、消費者団体のデモクラシー・技術センター（Center for Democracy and Technology）も個人情報の共有あるいは情報へのアクセスは「疑いのある特定の個人のみを対象に絞るべき」と強く主張している。しかし、国土安全保障という大義の下での個人情報共有は必要不可欠という声も多く、保守派からは「今後、よりよい個人情報共有に向けた解決策や手法を連邦政府が出していくべき」という意見が出されている[4][5]。

（ウ）連邦捜査局は地方団体と共有する捜査用データベースを構築予定

2004 年８月の大統領指令（上記参照）を受けた連邦捜査局（FBI：Federal Bureau of Investigation）は、2005 年より捜査用データベースを連邦政府と地方団体（州政府・地方自治体）の法執行機関同士で共有するネットワークの構築に着手している。この『地域データ交換（R-DEx：Regional Data Exchange）』ネットワークは、前出の『全国情報交換モデル（NIEM）』の姉妹版として、特に連邦捜査局が必要とする捜査情報を地方団体と全米レベルで共有することを目的としている。同ネットワークを利用することで、例えば「近い将来、化学プラント襲撃の可能性がある場合、連邦捜査局は地方団体の法執行機関より当該化学プラント周辺に住む人物情報を即座に入手する」ことができるなど、連邦捜査局の活動をより効果的・効率的に推進するために必要な情報により簡単にアクセスすることができるようになると期待されている。使用言語は XML ベースで、検索エンジンのグーグル（Google）と同様の検索機能も搭載する。

連邦捜査局は 2005 年２月、ミズーリ州セントルイス市周辺地区で同捜査用ネットワークの本格的運用に向けてパイロット・プログラムを開始した。ここでは、連邦捜査局、ミズーリ州高速警備隊、セントルイス市警察、セントルイス郡警察、並びにイリノイ州警察局とイリノイ州セント・クレア郡保安局の計７機関が共通のデータベースにアクセスして捜査情報を共有することに成功している。この成功を受けて、連邦捜査局は、2005 年８月１日より新たにワシントン州シアトル市周辺地区でもネットワークの試験的運用を開始しており、９月には更に 12 から 18 地域での展開も視野に入れている[6]。

---

[4] GOVEXEC.com 紙、2004 年 11 月９日。
http://www.govexec.com/dailyfed/1104/110904tdpm2.htm

[5] このような意見を出す主要機関としては、保守系技術政策シンクタンクのポトマック政策研究所（Potomac Institute for Policy Studies）が挙げられる。

[6] InfoWorld 紙、2005 年６月。
http://www.infoworld.com/article/05/06/30/HNfbinetwork_1.html

（エ）内国歳入庁／州政府間の納税者情報共有

財務省（DOT：Department of Treasury）内の内国歳入庁（IRS：Internal Revenue Services）は、2003 年 9 月 16 日より、全米 50 州政府と納税者情報を共有している[7]。『IRS 連邦・州政府プログラム（IRS Fed/State Program）』と呼ばれるこの施策は、連邦税の納税者情報を共有することで脱税者発見のための重複作業などを削減することを目指す。また、国民・企業・団体が税法を順守しているかを確認・支援する作業を迅速化し、さらには「顧客サービスの向上」も目指す。『IRS 連邦・州政府プログラム』で共有される納税者情報や根拠法などの概要は、表 1 の通りとなっている。基本的に、内国歳入庁と各州政府が同プログラム実施に当たって個別に契約を結び、その中で情報共有の対象となる個人情報や情報共有のタイミングなどが指定されている。

表 1　内国歳入庁『IRS 連邦・州政府プログラム』概要

目的	脱税者の発見
共有対象となる個人情報	• 連邦税確定申告書（Federal tax return） • 納税情報（return information）――納税者名、住所、納税番号、配偶者名、勤務先・勤務先住所、銀行口座情報など • 確定申告書が脱税調査の対象か否か • 内国歳入庁コンピュータシステム内の情報 • 確定申告提出状況 • 滞納状況　など
情報を共有する地方団体	全米 50 州政府
根拠法	• 内国歳入法 6103（d）節（Internal Revenue Code Section 6103（d））[8] • 関連州法（存在する場合）
内国歳入庁・州政府との契約など（州政府納税局が必要とした場合）	• 個別契約書 • 『脱税行為摘発のための覚書（Memorandum of Understanding Between Internal Revenue Service Small Business/Self-Employed Division（SB/SE） and [State tax agency] Concerning Abusive Tax Avoidance Transactions）』[9]
情報共有のタイミング	定期（月・四半期・年ごとなど） （契約で指定されていないタイミングで情報共有を求める場合は書面にて要求する）

出典：内国歳入庁ウェブサイト[10]

[7] 内国歳入庁 2003 年 9 月 16 日プレスリリース：
http://www.irs.gov/newsroom/article/0,,id=112866,00.html
[8] http://www.house.gov/jct/x-63-05.pdf
[9] ネバダ州、ワイオミング州以外の全米 48 州（Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin）及びワシントン DC、ニューヨーク市、米領バージン諸島、米領プエルトリコが署名。http://www.irs.gov/newsroom/article/0,,id=112870,00.html
[10] http://www.irs.gov/govt/liaisons/article/0,,id=133087,00.html

イ．カナダ

カナダ連邦政府と州・準州における個人情報の包括的な共有事例はなく、個々の連邦政府機関と州・準州とが個別に契約を締結し、個人情報を共有する事例がみられる。しかし、共有される個人情報は、移民データや、統計情報などの特殊なものに限定されている。

以下では、

・カナダ統計局・地方団体間の統計データ共有

・カナダ市民権・移民省、州政府間の移民データ共有

について取り上げている。

（ア）カナダ統計局／地方団体間（州政府統計局）の統計データ共有

カナダ統計局（Statistics Canada）は、国内統計を司る連邦機関であり、カナダ連邦政府で唯一、包括的な個人情報を収集する機関である。同局は、経済統計、社会統計、国土・市民全般の統計に至るまでのデータを収集・統合し、分析することが統計法（Statistics Act）によって義務付けられている。同法はまた、同局の任務遂行目的で他の政府機関が収集したデータを使用することを認めている。

このような中央集権型の統計システムのもと、カナダ統計局は、州や自治体といった地方団体と共同でデータを収集する『データ共有契約（Data-sharing agreements）』に基づき、国勢調査のような個人情報を含むデータをこれら地方団体と共有している。『データ共有契約』にて共有される統計データや根拠法などの概要は**表** の通り。

表 2　カナダ統計局『データ共有契約』概要

目的	統計調査作業の重複の回避と、それに伴う書類業務の削減
共有対象となる個人情報	国勢調査、企業調査など
情報を共有する公共団体	連邦機関、州政府、その他
根拠法	統計法（Statistics Act）[11]
情報共有のタイミング	随時共同調査が必要な場合
その他	調査の際に「共同調査を行っているためデータを共有する」ことに対する承認を必ず得る

出典：カナダ統計局ウェブサイト[12]

（イ）カナダ市民権・移民省／アルバータ州及びオンタリオ州の移民データ共有

カナダ市民権・移民省（CIC：Citizenship and Immigration Canada）は、『移民・難民保護法（Immigration and Refugee Protection Act）』[13]により、国内の州政府機関と移民関連の責任を共有することが認められている。

同法の下、カナダ市民権・移民省は、現在９州（アルバータ州、ブリティッシュ・コロンビア州、マニトバ州、ニューファンドランド・ラブラドール州、ノバスコシア州、オンタリオ州、プリンス・エドワード・アイランド州、ケベック州、サスカチュ

[11] http://www.statcan.ca/english/about/statact.htm
[12] http://www.statcan.ca/english/survey/business/sharing.htm
[13] http://www.cic.gc.ca/english/irpa/index.html

ワン州）並びにユーコン準州のそれぞれの州政府と、移民関連業務について共同責任を負うとする契約書（連邦―州・準州契約（Federal-Provincial/Territorial Agreements））[14]を締結している。例えば、アルバータ州は、2003 年９月８日、お互いが保有する移民情報を交換することに同意した覚書『カナダ―アルバータ州における情報共有覚書（Canada-Alberta Memorandum of Understanding on Information Sharing）』[15]をカナダ市民権・移民省と締結した。同様に、2004 年３月、オンタリオ州も情報共有覚書『2004 年カナダ―オンタリオ州における情報共有覚書（Canada-Ontario Memorandum of Understanding on Information Sharing – 2004）』[16]を結んでいる。

カナダ市民権・移民省と州政府が共有する個人情報の概要は**表** に示す通りとなっている。

表 3　カナダ市民権・移民省と州政府が共有する個人情報の概要

共有対象となる個人情報	連邦政府から州政府へ提供	州政府から連邦政府へ提供
	a. 事業登録番号（Federal Client Identification Number）、あるいは書類番号（Document Identification Number） b. 氏名 c. 生年月日 d. 性別 e. 直近の住所 f. 直近の電話番号 g. 既婚の有無 h. カナダ入国日あるいは到着日 i. カナダ到着日あるいは永住権取得日 j. 永住権カテゴリー k. 永住権申請状況 l. 永住権保証人情報（保証人がある場合） m. 保証人失効通知（失効した場合） n. 就労許可証（申請済みの場合） o. 就学許可証（申請済みの場合） p. 財務状況 q. その他財務支援書類	a. 州の個人登録番号（Provincial Person Identification Number） b. 氏名 c. 生年月日 d. 性別 e. 直近の住所 f. 直近の電話番号 g. 既婚の有無 h. 生活保護を受けている場合その情報 i. 保証人が失効した場合の返金状況 j. その他収入 k. 直近の雇用主の氏名・住所 l. 財務状況
情報共有のタイミング	双方からの要求があった場合	

出典：オンタリオ州、アルバータ州覚書

[14] http://www.cic.gc.ca/english/policy/fedprov.html
[15] http://www.cic.gc.ca/english/policy/fed-prov/can-alberta-mou.html
[16] http://www.cic.gc.ca/english/policy/fed-prov/ont-mou-2004.html

（2）公共団体が共有する個人情報ネットワークシステム及び地域住民との情報共有

ア．米国

米国公共団体における個人情報の共有は、防犯を目的とした犯罪者情報の共有事例のみであり、住民基本台帳のような一般市民の情報を共有する事例はみられない。同様に、このような個人情報を地域住民と共有する事例についても一部地域で性犯罪者情報を開示する他はみられない。

以下では、地方団体間で犯罪者情報を共有している例として、ワシントン州内の市警察の試みを取り上げるほか、地域住民との情報共有が進んでいる性犯罪者情報について簡単にまとめている。

（ア）地方団体間での犯罪者情報共有

ワシントン州キング郡警察は、同郡内のベルビュー市とタクウィラ市警察における犯罪者情報をリアルタイムで共有するデータ共有ネットワークを構築している（どのような個人情報が管理・共有されているかについての詳細は非公開である）。

『地域情報自動ネットワーク（RAIN：Regional Automated Information Network）』と呼ばれるこのシステムは、マイクロソフトウィンドウズ OS をベースとしたマイクロソフト・SQL サーバ 2000 に蓄積するデータベースにベルビュー市とタクウィラ市警察職員のうち 1,300 名のエンドユーザがアクセスしている。今後、『RAIN』は最大 39 の警察署に導入され、デスクトップ PC の他、巡回車両（パトカー）や PDA、携帯電話からのアクセスも可能となる予定である[17]。

（イ）地域住民との情報共有

米国では、地域によっては性犯罪者情報を地域住民に公開して再犯を防ぐ措置を取っている。一方で、地方団体が所有・管理する一般の個人情報を地域住民と共有するといった事例はみられない。

性犯罪者情報を公開している地方団体の例としてフロリダ州がある。同州では、フロリダ法執行省（Florida Department of Law Enforcement）が性犯罪者のデータベースを作成しており、データベースは公式ウェブサイト

＜http://www3.fdle.state.fl.us/sopu/index.asp＞で閲覧可能であるほか、通話料無料の電話番号にかけることで、地域に住む性犯罪者情報を得ることができる。

オンラインデータベースは、フロリダ州居住者以外でも閲覧することができるもので、フロリダ州に住む性犯罪者を「氏名」「郡」「市」「郵便番号」といった条件から検索できる。2005 年 11 月 21 日現在でタンパ市に居住する性犯罪者を検索したところ 953 名の情報が得られ、それぞれの犯罪者につき以下が公開されている。

[17] マイクロソフト社ウェブサイト。
http://www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=15362

- 顔写真
- 氏名
- 氏名以外に利用してきた偽名
- 誕生年月日
- 人種
- 性別
- 髪の色
- 目の色
- 身長
- 体重
- 身体的特徴（傷跡、刺青など）
- 最新の住所
- 当該住所への移転年月日
- 性犯罪内容　等

米国では、このように性犯罪者や児童虐待者の情報を地域住民と共有することで、地域における防犯意識が高まることが期待されている。

イ．カナダ

カナダの公共団体が共有する個人情報ネットワークシステムや、地域住民との情報共有の仕組みは、今回の調査では見られなかった。

（3）住民番号制度の概要及び取扱い状況

米国及びカナダでは、国家統一的な住民番号制度を採用していない。一方で、両国とも、年金などの社会保障を受けるための登録番号である「社会保障番号」が、税務や選挙人登録、銀行口座開設、運転免許証取得などにおける本人確認番号として広く採用されている。以下に、米国及びカナダにおける社会保障番号制度の概要とその取扱い状況を纏める。

ア．米国

米国の社会保障番号（SSN：Social Security Number）は、本来は社会保障を受けるための登録番号と納税のための登録番号の両方の役割を果たすものとして発行されてきた番号であったが、戸籍制度をとらない米国において唯一の個人確定（身分証明）の役割も果たすようになっている。

（ア）社会保障番号（SSN）概要

社会保障番号は、米国民並びに移民や米国政府に納税する外国人に対して無料で発行され、一度発行された番号は無期限で使用できる。

米国籍を保有する米国民の場合、出生証明書を申請する際に同時に社会保障庁（SSA：Social Security Administration）に申請するか、あるいは年齢と身元を証明できる書類と共に申請する。また、子供を税控除対象として確定申告するためには、満 1 歳以上の子供の社会保障番号を必ず取得することが義務付けられている。なお、米国で生まれ米国籍を持つものが 12 歳以上で初めて社会保障番号を申請する場合、「なぜ出生時に番号を申請しなかったか」といった面接を受ける必要がある。

米国籍を持たない者や移民の場合、身元を証明する書類（パスポートや戸籍、出生証明書など）と共に申請し、国土安全保障省で身元が確認されると番号が発行される。なお、米国籍を持たない者で労働を許可されないビザの所持者（学生ビザ、配偶者ビザなど）に対して社会保障番号は発行されない。

社会保障番号は、同番号と氏名を記した紙製のカード『ソーシャル・セキュリティ・カード（Social Security Card）』（画像右参照）として発行される。カードの種類は以下３種類で、それぞれカード所有者の米国内の就労許可状態を示している。

出典：カリフォルニア大学バークレー校
http://www.berkeley.edu/news/media/releases/2005/01/28_socsec.shtml

・名前と社会保障番号のみ：米国籍市民、あるいは合法的に就労できる外国籍の市民
・氏名、番号のほか但書「国土安全保障省が承認する場所のみで就労可能」[18]のあるもの：合法的に米国に一時滞在する者で、就労許可を得た外国籍の市民
・氏名、番号のほか但書「就労不可」[19]のあるもの：合法的に米国に一時滞在する者で、就労許可がない外国籍の市民

社会保障番号は、９桁の数字で、以下の３つの構成要素で成り立っている（XXX-XX-XXXX）。

・最初の３桁：郵便番号ごとに区分けされた地域番号[20]。
・中２桁：「グループ番号」と呼ばれ、奇数・偶数の数字で組み合わされる。１桁目が奇数・２桁目が偶数の番号をすべて使い切ると、１桁目が偶数・２桁目が奇数の番号が割り当てられる。
・下４桁：通し番号。0001 から 9999 まで通しで発行される。

（イ）社会保障番号（SSN）取扱状況

社会保障番号は、社会保障受給目的で 1936 年に発行されて以来、現在では住民番号に近い位置づけで利用されてきている。具体的には、企業での従業員管理や病院でのカルテといった医療記録管理や健康保険口座管理目的で提供が求められる他、クレジットカード、銀行口座開設、運転免許証取得の際に提供が求められる。また、高校や大学での学生番号や、企業の従業員番号としてそのまま利用される場合もある。

このように、社会保障以外で広く利用されている背景として、記録管理媒体が紙からコンピュータに移行した際、地域や通し番号で構成される社会保障番号がコンピュータ管理において利便性が高かったことが大きな要因として考えられている。

a　個人情報保護の観点からの法規制

現在、個人情報保護の観点から、社会保障番号の広範な利用は控えられる傾向にある。例えば、『1974 年プライバシー法（Privacy Act of 1974）』[21]（1975 年１月施行）第７節（a）（１）では、すべての公共団体（連邦、州、地方自治体）に対し、個

[18] “VALID FOR WORK ONLY WITH DHS AUTHORIZATION”
[19] “NOT VALID FOR EMPLOYMENT”
[20] 1972 年までは社会保障番号を発行した社会保障庁の地域分室によって番号が区切られていた。現在の最初の３桁の配分一覧：http://www.ssa.gov/foia/stateweb.html
[21] http://www.usdoj.gov/foia/privstat.htm

人から社会保障番号を受け取る際はその番号の取扱い方法などを明示することを定めている。具体的には以下の通り。

・個人が社会保障番号の提示を拒否しても、連邦・州政府及び地方自治体は当該個人に対して、法の下の権利を享受することを拒否してはならない
・連邦・州政府及び地方自治体が個人に対し社会保障番号の提示を求める際は、その要請が義務的あるいは自主的なものであるかという点、また利用方法やその根拠となる権限（法規制）を明示する

その他、社会保障番号を含む個人情報一般の取扱いについては、個人情報保護に関する連邦法・州法にて定められている（個人情報保護についての詳細は、『第３章：個人情報保護・情報セキュリティ対策』参照）。

イ．カナダ

カナダも米国同様に住民番号制度を採用せず、社会保障番号（SIN：Social Insurance Number）が個人確定（身分照明）の役割を果たしている。カナダの社会保障番号は、カナダ政府社会保障、並びに各種厚生年金受給者の口座番号として 1964 年より配布されているもので、1967 年よりカナダ歳入庁（CRA：Canada Revenue Agency）が納税者番号としても採用を始めている。後述のとおり、社会保障番号の利用は法によって規定されているため制限されているが、企業の多くが雇用の際などに身分証明として社会保障番号の提示を求めることが多い。

（ア）社会保障番号（SIN）概要

カナダ国内外で出生したカナダ国民の場合は出生証明書（海外で出生した場合はカナダ市民権・移民局の承認が必要）、永住者は永住カードその他書類、並びに短期滞在者は就労許可証などを提出して番号を申請する。移民・難民の場合は、カナダ国内での就労許可がある者に限り、社会保険番号を申請することができる。社会保険番号は、一度取得したら永久的に同じ番号を保有することが出来る。なお、2004 年４月４日以降、短期滞在者向けの社会保険番号に限り有効期限が設定された（この場合番号は「９」から開始する）。

出典：カナダ社会開発省
http://www.sdc.gc.ca/asp/gateway.asp?hr=en/cs/sin/010.shtml&hs=sxn

社会保険番号は、同番号と氏名を記したプラスチック製カード『SIN カード（Social Insurance Number Card）』（画像左参照）として無料（再発行の場合は 10 カナダドル）で発行される[22]。

[22] カナダの社会保障番号が示す情報については公開されていない。しかし、例えばインターネット検索をするとその解読方法などを載せた個人のウェブサイトなども多く見られる。

（イ）社会保障番号（SIN）取扱状況

カナダの社会保障番号は、カナダ法[23]に基づき、カナダ国民に対し取得を義務付けている。また、個人の納税情報を必要とする機関（雇用主、銀行、信用組合など）に対しても、社会保障番号の提示が義務付けられる。以下**表** は、社会保障番号を個人管理に利用することが認められている主な機関・施策である。

表 4　社会保障番号を個人管理に利用することが認められている主な機関・施策

主な機関・施策
カナダ年金基金（CPP）、老齢年金（OAS：Old Age Security）、所得比例年金
所得税の確定申告
銀行、信託銀行、証券ブローカー（利息に対する所得税確定申告用書類作成）
退役軍人向け福利厚生施策
カナダ政府学生金融支援施策（Canada Student Loans, Canada Student Financial Assistance）
カナダ政府教育奨学金（Canada Education Savings Grants）
ガソリン、飛行機燃料物品税申告
カナダ小麦委員会法（Canadian Wheat Board Act）[24]
労働調整福利厚生法（Labor Adjustment Benefits Act）
税還付割引規制（Tax Rebate Discounting Regulations）
競馬関連規制（Race Track Supervision Regulations）
債務差し押さえ関連規制
カナダ選挙法（Canada Elections Act）
カナダ労働法典（Canada Labour Code）
農業収入保護法（Farm Income Protection Act）

出典：カナダ・プライバシー・コミッショナー室ウェブサイト[25]

一方で、社会保障番号は、上記以外の場合においても、本人確認などの理由で提示を求められてきたが、近年の個人情報保護の動きに伴い、カナダ政府は個人に対して社会保障番号を提示する際の注意をウェブサイトなどで呼びかけている[26]。また、カナダの地方団体（州政府、地方自治体など）も、個人から社会保険番号情報の入手・使用が禁止されてはいないものの、各地方団体にて自主規制を行っている場合が多いという。

[23] 社会保障番号取得を義務付けるカナダ法一覧：
http://www.sdc.gc.ca/asp/gateway.asp?hr=/en/cs/sin/075.shtml&hs=sxn
[24] 国営貿易企業のカナダ小麦委員会（CWB：Canadian Wheat Board）の根拠法。
[25] http://www.privcom.gc.ca/fs-fi/02_05_d_02_e.asp
[26] 社会保障番号の提示が義務付けられている機関などの情報（カナダ・プライバシー・コミッショナー室（Office of the Privacy Commissioner of Canada））：http://www.privcom.gc.ca/fs-fi/02_05_d_02_e.asp
SIN カードの盗難・紛失の際の手続きなど（カナダ社会開発省）：
http://www.sdc.gc.ca/asp/gateway.asp?hr=/en/cs/sin/125.shtml&hs=sxn

2　公共団体が発行する IC カードの導入・計画状況

米国、カナダにおける全国一律で発行する IC カード（あるいは『スマートカード（Smart card）』）のうち、ある程度大規模な導入、あるいは導入が計画されているものとして、米国の連邦政府職員を対象にした ID カードと一部地域限定の公共交通パスの IC 化の実用例がある。

（1）連邦・地方団体における IC カード発行の実態

ア．米国

米国の連邦政府機関は従来、各省庁が独自の技術・方法で、個人情報を含めた IC カードの開発・発行を行ってきた。このような中、2004 年 8 月 27 日にブッシュ大統領が、連邦政府職員及び契約職員すべてを対象にした省庁横断型の ID カード（IC カード）の導入を義務付けたため、各省庁がこれに従うことが求められている。以下では、連邦政府における ID カードについて詳細を纏める。

ａ．　連邦政府職員 ID カードの「連邦 ID スマートカード」

連邦政府機関は従来、省庁ごとに傘下の職員を対象にした入館用の ID カードを作成してきた。例えば国防総省（DOD：Department of Defense）は、2000 年 10 月 10 日より、同省の職員、軍職員、その他契約社員などを対象にした入館用 ID カードを、新たに接触型スマートカード『共通アクセスカード（CAC：Common Access Card）』（画像右参照）に切り替えている。同カードは、入館目的の他、PC アクセスへも利用される。全メモリー容量 32 キロバイトのうち、25 キロバイトまで各自好きな情報を保存することができる[27]。2004 年からは『次世代 CAC カード』として、メモリー増量、非接触型機能、バイオメトリクス読取り機能なども搭載予定としている。

出典：国防総省プレスリリース
http://www.defenselink.mil/news/Oct2000/n10102000_200010107.html

①大統領指令による省庁横断型 ID カードの構築

このように各省庁がバラバラに ID カード発行を実施している中、ブッシュ大統領は 2004 年 8 月 27 日、連邦政府職員と連邦政府下請け業者に対し、共通で利用できる ID カードの発行を求めた大統領指令『国土安全のための大統領指令 Hspd-12（Homeland Security Presidential Directive）』[28]を発行した。この大統領指令では、政府機能の効率化のほか、連邦政府職員をテロから守り、また個人情報盗難も防止することを目的としている。これに向け、商務省（DOC：Department of Commerce）

[27] 国防総省の『共通アクセスカード』に搭載される具体的な個人情報は開示されていない。
[28] http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

に対し、省庁横断型 ID カードの仕組みを構築するための技術標準の作成を、国務省（DOS：Department of State）、国防総省、国土安全保障省や、大統領府行政管理予算局（OMB：Office of Management and Budget）などと協力して行うことを義務付けた。また、技術標準作成後、以下のようなスケジュールに沿って、各連邦省庁は ID カードを導入することも決められた。

・技術標準公布後４ヶ月以内に、各連邦省庁長官は、技術標準に沿った ID カード実装計画を必ず作成する。
・技術標準公布後８ヶ月以内に、各連邦省庁長官は、技術標準に沿った ID カードの採用を開始する。

大統領指令を受けた商務省国立標準技術研究所（NIST：National Institute of Standards and Technology）は、大統領指令発表から僅か６ヵ月後の 2005 年２月 25 日、省庁横断型 ID カードの技術標準『FIPS（Federal Information Processing Standard）-201』[29]を発表した。この技術標準は、第一部（人物特定、セキュリティ、プライバシーに関する共通の必要条件）と第二部（非接触型、バイオメトリクス技術採用といった、詳細な技術仕様）から構成されている。技術標準の作成・調整に当たっては、商務省国立標準技術研究所の情報技術研究所（ITL：Information Technology Laboratory）が担当機関となり、技術標準の最終承認は商務省長官が行った。

その後 2005 年４月１日、行政管理予算局（OMB）がより詳細な連邦 ID カード導入に向けた計画指針（guidance）[30]を以下**表** の通り発表した。これによると、技術標準『FIPS-201』第一部の採用を 2005 年 10 月 27 日に、第二部の採用を 2006 年 10 月 27 日までに完了することが求められている。

[29] http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
[30] http://www.whitehouse.gov/omb/inforeg/hspd-12_guidance_040105.pdf

表 5　行政管理予算局による連邦 ID カード導入指針

期限	対象省庁		
	商務省	総務庁[31]	連邦 ID カード 採用対象省庁
2005 年			
2 月 25 日	• 技術標準『FIPS-201』発表		
3 月 14 日		• 『FIPS-201』順守のベストプラクティスを纏めた手引き『連邦アイデンティティ管理手引き（Federal Identity Management Handbook）』[32]発行	
4 月 29 日	• より詳細な技術仕様公布[33]		
6 月 25 日	• 技術標準の参考実装（reference implementation）を公布		
6 月 27 日			• 技術標準導入計画を行政管理予算局に提出
7 月 31 日		• 技術標準順守のために調達する物品・サービスも、技術標準に順守することを確認するための手続き（process）を構築	
8 月 5 日	• 実証実験（conformance testing）報告		
8 月 27 日			• 連邦 ID カードを利用する可能性のある、連邦政府所有建築物の特定
10 月 27 日		• 技術標準順守を盛込んだ連邦調達規定（FAR：Federal Acquisition Regulation）修正版を発行（予定）	• 技術標準第一部順守（予定）
2006 年			
10 月 27 日			技術標準第二部順守（予定）

出典：行政管理予算局連邦 ID カード導入に向けた計画指針[34]

[31] GSA（General Services Administration）
[32] 『連邦アイデンティティ管理手引き（Federal Identity Management Handbook）』：http://www.cio.gov/ficc/documents/FedIdentityMgmtHandbook.pdf
[33] http://csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf
[34] http://www.whitehouse.gov/omb/inforeg/hspd-12_guidance_040105.pdf

②省庁横断型 ID カードの課題

コンピュータ関連ハードウエア、ソフトウェア・ベンダーで構成される、米国最大の情報技術業界団体の ITAA（International Transactional Analysis Association）は 2004 年 12 月 22 日、国立標準技術研究所が発表した技術標準『FIPS-201』の仕様の見直しを迫る発表を行った[35]。ITAA は、このような連邦政府における ID カード統一に向けた動きは、既に何らかの形で ID カードを独自に発行している省庁の取り組みや、個人情報管理を進めようとする省庁横断型の動きなどをまったく無視している点を指摘し、国立標準技術研究所に対し①技術標準第一部順守期日の延期、②行政管理予算局と共同で技術標準順守計画と予算を作成、③既に省庁横断型で行われている個人情報管理への動きを反映させる、の 3 点を要望した。

更に ITAA は 2005 年 2 月 15 日、既に独自の ID カードを発行している連邦省庁とそうでない省庁間では、『FIPS-201』に順守する ID カードの発行の難しさが異なるとの見解も発表している[36]。ITAA によると、例えば国防総省など既に独自のカードを発行している省庁は、採用ベンダーともに『FIPS-201』順守への対応期間とコストが大きくなるという。

ITAA 同様、既に ID カードを作成している省庁からも、国立標準技術研究所の技術基準『FIPS-201』を順守することが難しいとして、大統領指令に反対の声が挙がっている。例えば国防総省国防人的資源データセンター（Defense Manpower Data Center）ディレクター、マリー・ディクソン氏（May Dixon）によると、同省が既に発行・利用している『共通アクセスカード（CAC）』400 万枚のうち、2005 年 5 月の時点で 8 割が『FIPS-201』に順守できているものの、残り 2 割の順守は 2009 年にずれ込むとの見込みが強いとし、行政予算管理局が定める導入計画遂行の難しさを訴えている[37]。また、『FIPS-201』では、連邦政府職員以外に、契約社員の身元調査も義務付けているため、連邦職員の身元調査を担当する連邦人事管理局（OPM：Office of Personnel Management）は、大統領指令施行後に大量の身元調査を行うことになるため、大幅な業務の増加とそれに伴うコスト増を危惧している[38]。

このように、連邦政府統一型 ID カードを早期に導入することを目指した大統領指令は、ID カード・システムを実際に構築する IT 業界や、実際に運用する連邦省庁機関から強い反対を受けている。米国では、大統領指令であっても、業界団体からの圧力などから、その施行が停止することも起こり得るため、連邦省庁横断型の ID

[35] ITAA プレスリリース、2004 年 12 月 22 日。
http://www.itaa.org/eweb/Dynamicpage.aspx?webcode=PRTemplate&wps_key=8f7b4cd7-8cf6-47d7-9b55-62382050c4ed&wps_key=8f7b4cd7-8cf6-47d7-9b55-62382050c4ed
[36] ITAA プレスリリース、2004 年 2 月 15 日。
http://www.itaa.org/eweb/Dynamicpage.aspx?webcode=PRTemplate&wps_key=4180dd25-64ed-433d-840c-6c0cac3f0510&wps_key=4180dd25-64ed-433d-840c-6c0cac3f0510
[37] GCN 紙、2005 年 4 月 5 日。
[38] Federal Computer Week 紙、2005 年 9 月 13 日

カードの導入は、行政管理予算局が示す計画通りには進まない可能性も高くなっている。

イ．カナダ

永住権を取得した移民を対象に、出入国管理目的で IC カードが発行されている。しかし、このような公的団体が全国一律に発行している IC カードプロジェクトは、調査時点では存在しない。

（２）公共交通パスの IC 化

米国、カナダ両国における公共交通パスの IC 化事例は、いずれも全国一律に発行されたものではない。しかし、以下では、地理的にも広範域を対象としている２例（ワシントン DC 首都圏交通網 IC カードと、トロント大都市圏交通網共通 IC カード）について、参考情報として取り上げる。

ア．米国

全米レベルで一律に発行された公共交通パスではないものの、比較的広範囲で利用されているのが、ワシントン DC 首都圏交通網 IC カードである。同カードは現在、大手クレジットカード会社と提携して、クレジットカードに公共交通パス機能を備えるサービスも開始している。

（ア）ワシントン DC 首都圏交通網 IC カード

ワシントン DC 首都圏の地下鉄・バスを運営するワシントン首都圏交通公社（WMATA：Washington Metropolitan Area Transit Authority）[39]は、1999 年５月より非接触型 IC カード『スマートリップ（SmarTrip）』を採用している。同公社は 1967 年に設立され、現在の年間輸送人数は３億 3,600 万名（地下鉄１億 9,000 万名、バス１億 4,600 万名）に上る。

『スマートリップ』はプラスチック製で、一枚５ドルで販売されている。最大 300 ドルまでの入金（チャージ）機能が搭載されており、同じカードを繰り返し使用することができる。ワシントン首都圏交通公社が運営する地下鉄、バスで利用でき、一方で既存の紙製の切符や回数券、定期券なども引き続き使用されている。さらに、各地下鉄の駅に隣接する同公社運営の駐車場の支払い方法も、2004 年６月 28 日より『スマートリップ』のみとなっている[40]（下写真は、バスにおける『スマートリップ』使用方法）。

ワシントン首都圏交通公社によると、『スマートリップ』発行枚数は 2005 年５月 20 日に 100 万枚を達成し、通勤ラッシュ時の利用者の６割が既に同カードを所有して

[39] ワシントン首都圏交通（WMATA：Washington Metropolitan Area Transit Authority）：http://www.wmata.com/

[40] ワシントン首都圏交通ウェブサイト。http://www.wmata.com/riding/smartrip.cfm

いるという[41]。『スマートリップ』購入時に、ワシントン首都圏交通公社のウェブサイトから『スマートリップ』番号と氏名を登録すると、『スマートリップ』を紛失しても再発行が可能である。

出典：ワシントン首都圏交通公社（WMATA）
http://www.wmata.com/riding/SmarTrip_fullrolloutF

更に、2004 年５月より、大手金融機関のシティ・グループ（Citi Group）が発行するクレジットカード『Citi Cards』に、非接触型交通パス IC カード機能を合体させたパイロット・プログラムが実施されている。同カードは、『スマートリップ』と、クレジットカード（マスターカード）の両方の機能を利用することが出来る。30 ヶ月間限定で実施されるこのプロジェクトは、『Citi Cards』に申し込んだ顧客に対し、申し込み後６ヶ月以内の期間であれば、ワシントン首都圏交通公社運営の地下鉄・バス・駐車場での支払いが５％割引となるキャンペーンも実施している（最大 300 ドルまで）。同パイロット・プログラム実施におけるワシントン首都圏交通公社の支出はなく、すべてシティ・グループが負担している。

イ．カナダ

カナダも、米国同様、全国レベルで一律に発行された公共交通パスの事例はない。一方で、オンタリオ運輸省が主導となり、複数の都市を結ぶ複数の交通公社にて共通で利用できる IC カードの発行を目指したプロジェクトが始動している。

（ア）トロント大都市圏交通網共通 IC カード

トロント大都市圏交通公社（GTTA：Greater Toronto Transit Authority）、通称『GO トランジット（GO Transit）』は現在、2007 年初頭を目処に公共交通パスの IC 化を目指し、オンタリオ運輸省（MTO：Ontario Ministry of Transportation）主導のプロジェクトを展開している。同プロジェクトは、トロント周辺都市圏（GTA：Greater Toronto Area）を結ぶ地域一帯（人口 550 万人、8,100 平方キロメートル、画像右参照）を対象に、複数の交通機関のバ

出典：オンタリオ運輸省
http://www.mto.gov.on.ca/english/traveller/fare

[41] ワシントン首都圏交通プレスリリース、2005 年５月 20 日。
http://www.wmata.com/about/MET_NEWS/PressReleaseDetail.cfm?ReleaseID=795

スや電車などで共通で利用できるICカード『GTAフェアカード（GTA Farecard）』を発行するものである。参加する交通機関の利用者数は、年間で5億 2,600 万名を超える。

2005年4月にベンダーからのRFQ（Request For Qualifications、資格要請）を受け、IC カード・システム構築ベンダー候補を4社に絞り、現在はこれら4社から設計やシステム構築などの RFP（Request for Proposal、提案依頼書）提出を要請している。2006 年初頭には、システム構築ベンダーを決定し、2007 年初頭には採用システムを決定する計画となっている。そして、システム導入は 2008 年初頭より開始し、トロント周辺都市圏全域への導入は2010年に完了予定である。

第２節　公共団体が個人を対象にした電子認証サービス（公的個人認証サービス）の展開

１　公的個人認証サービスの現状

米国では、『E-Authentication（電子認証）』イニシアチブや政府間での相互認証局『連邦相互認証局（FBCA：Federal Bridge Certification Authority）』といった複数の取組みが進められているが、調査時点においても、全ての省庁を対象とした統一の電子認証基盤はない。一方のカナダは、全国レベルで実施する電子認証プロジェクトが主体となり、連邦省庁と州・準州間での相互認証も実現している。

（１）連邦政府における政策、連邦法、経緯、推進機関及びサービス提供機関

ア．米国

米国では、連邦省庁間での相互認証を可能にするシステム設計を行うことを目的とした『E-Authentication』イニシアチブが 2003 年より立ち上がっているが、現時点では実現の見通しは立っていない。

（ア）E-Authentication（電子認証）

米国連邦政府が推進する 25 の電子政府プロジェクトの一環として、2003 年7月3日『E-Authentication（電子認証）』イニシアチブが立ち上がった。同イニシアチブは、連邦政府機関の電子政府を利用する個人を対象に、シングル・サインオンですべての電子政府サービスを利用できるように、省庁間での相互認証を可能にするシステム設計を行うことを目的としている。主導組織は総務庁（GSA：General Services Administration）である。

『E-Authentication』イニシアチブ発足の背景として、①連邦政府機関がそれぞれ独自に電子認証を行っていることに伴う認証の重複作業による損失が大きく、例えば 2003 会計年度から 2004 会計年度にかけて、このような損失額が1億 6,000 万ドルに上ったこと、②各連邦省庁がそれぞれ独自に物理的セキュリティやコンピュータ・セキュリティ対策をとっているため、利用者や連邦政府の安全がリスクに晒されている

こと、③各連邦省庁が採用する電子証明書がそれぞれ異なるためそれらを利用する米国市民へ負担が大きくなっていること、の３点が挙げられている[42]。

『E-Authentication』イニシアチブでは、連邦政府省庁共通の包括的な電子認証政策を構築するためにイニシアチブ発足後に立ち上げられた委員会『連邦個人認証委員会（FICC：Federal Identity Credentialing Committee）』を通じて省庁横断型の認証技術（スマートカード、電子認証など）の構築や、公開鍵基盤への投資の統合なども呼びかけている。現時点での成果として、同イニシアチブが認証するサービス・ベンダー・リストや技術ベンダー・リスト、リスク・アセスメントの手引き、技術アーキテクチャの完成が挙げられる。しかし、同イニシアチブの目指す相互認証の実現には、まだ時間を要するとの見方が現在では強い（現時点の動向・課題については本節の「３　公的認証システムの課題と政策の方向性及び今後の見通し」参照）[43]。

イ．カナダ

カナダ政府では、すべての政府機関を対象とした公開鍵基盤の構築に向けて 1999 年より取り組みが行われており、2002 年より公開鍵基盤サービスの『epass』を実用化している。

（ア）epass

カナダ政府は、電子政府イニシアチブ『GOL：Government On-Line』の一環として 1999 年５月 27 日、『カナダ政府における公開鍵基盤管理に関する規約（Policy on Public Key Infrastructure Management in the Government of Canada）』（通称：『政府 PKI 規約（Government PKI Policy）』）[44]を発行し、『カナダ政府 PKI』として公開鍵基盤の構築を進めてきた。以下**表** は、カナダ政府 PKI プロジェクトにおける組織構成である。

[42] http://www.cio.gov/eauthentication/documents/mf_memo7303.pdf
[43] Network World 紙、2001 年 10 月 11 日。
[44] http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki1_e.asp

表 6　カナダ政府 PKI 組織構成

組織	役割
管轄機関	
カナダ財務委員長 President of the Treasury Board of Canada	カナダ政府を代表するカナダ政府 PKI の総責任者。
カナダ財務委員会事務局 Secretary of the Treasury Board of Canada	カナダ財務委員長を補佐し省庁間での相互認証、連邦政府における PKI 管理の方向性を定める。
政策管理局 Policy Management Authority	カナダ財務委員長及び事務局に対し、PKI の戦略的方向性などを提言する、上級委員会。
運用機関	
認証局 Certification Authority	電子証明書の発行など、PKI の運営を行う第三者機関。連邦省庁自身が認証局を運営することも可能。ひとつの連邦省庁で複数の認証局を設置する場合もある。
地域登録局 Department Local Registration Authorities	PKI を利用する個人あるいは政府機関の本人認証作業を行う。
カナダ連邦 PKI ブリッジ Canadian Federal Public Key Infrastructure Bridge	省庁間あるいは省庁と認証局における関係強化、あるいは相互認証を行うための橋渡し業務を行う。
カナダ・セキュリティ確立 Canadian Security Establishment	カナダ連邦 PKI ブリッジを運営。

出典：カナダ公共事業・政府業務省

カナダ政府 PKI は 2002 年より、公開鍵基盤を利用した個人認証サービス『epass（イーパス）』を開始した。カナダ電子政府イニシアチブ『GOL』は、ウェブサイトへのオンライン・アクセスを、①公共情報へのアクセス、②オンラインでの書類記入、③オンラインでの個人情報の更新、という３つのセキュリティ・レベルに分類しているが、『epass』は「②オンラインでの書類記入」または「③オンラインでの個人情報の更新」のセキュリティ・レベルが設定されているウェブサイトへのアクセスにおいて利用されるツールである。なお、『GOL』は、2005 年までにすべての連邦省庁に『epass』を導入することを目標に掲げている。『epass』のより具体的な利用方法については、P23（１）個人認証システムの概要、用途、普及状況を参照されたい。

（２）地方団体における政策、連邦法、経緯、推進機関及びサービス提供機関

ア．米国

米国の地方団体における個人を対象にした電子署名プロジェクト事例はほぼ見当たらないのが現状である。このような中、イリノイ州における州内外の個人を対象にした電子署名プロジェクトがある。

（ア）イリノイ州電子署名プロジェクト

米国中西部に位置するイリノイ州（州都：スプリングフィールド市、最大都市：シカゴ市）の州政府は、2004 年より州内外の個人も対象にした電子署名プロジェクト

『イリノイ州政府 PKI』を実施している[45]。採用ベンダーは、政府向け電子個人認証・アクセス管理ソリューション・プロバイダのエントラスト社（Entrust）である。同州の電子証明プロジェクトは、最初に登録して公開鍵基盤を取得すれば、すべての州政府関連書類へオンラインでアクセスし、本人認証や電子署名の認証などが行える仕組みである。以下**表** は、イリノイ州政府 PKI プロジェクトにおける組織構成である。

表 7　イリノイ州政府 PKI プロジェクト組織構成

組織	役割
管轄機関	
中央管理サービス局 Department of Central Management Services （CMS）	イリノイ州電子商取引セキュリティ法 25-105 節（Illinois Electronic Commerce Security Act, Section 25-105）により、電子署名の発行、利用に関する認証規約（Certificate Policy）及び認証局運用規定（Certification Practices Statement）の作成権限を持つ。
中央管理サービス局長 Director of CMS	認証規約局による、認証規約及び認証局運用規定の導入・維持に関する総責任者。
運用機関	
認証規約局 Certificate Policy Authority （PA）	認証規約及び認証局運用規定の作成、導入、維持、改正、及びこれらにて義務付けられるすべての任務を遂行する。局員は、中央管理サービス局長により、イリノイ州政府職員の中から任命・解任される。
運用局 Operational Authority （OA）	認証規約及び認証局運用規定認証に沿って、規約局の作成する認証規約の解釈、認証局運用規定の作成・管理、イリノイ州 PKI の運用を行う。監督責任者は中央管理サービス局長。
中央管理サービス局（CMS） セキュリティ管理者 CMS Security Administrator	イリノイ州 PKI の運用監督責任者。
中央管理サービス局（CMS） 登録局 CMS PKI registration authority （RA）	イリノイ州 PKI の運用管理。
PKI 管理者 PKI Administrators	認証局業務。
地方登録局 Local Registration Authorities （LRAs）	中央管理サービス局（CMS）の業務を行う場合がある。

出典：イリノイ州 PKI 認証局運用規定[46]

『イリノイ州 PKI』のより具体的な利用方法は、P23「（1）個人認証システムの概要、用途、普及状況」で詳説する。

[45] イリノイ州政府は、連邦政府省庁がそれぞれ展開する電子認証システムと相互認証を目指した、最初の事例でもある。同州政府は 2001 年 5 月より、州政府と連邦政府に同じ書類を提出する業務（納税など）を対象に電子証明書の発行を開始している。具体的には、州内で事業を行い州税と連邦税を納める法人や、メディケイド（医療扶助）、メディケア（高齢者向け医療保険制度）を州政府及び連邦政府に申請する医療機関などが対象となっている。

[46] http://www.illinois.gov/pki/cps.cfm

イ．カナダ

カナダは、連邦レベルでの電子政府プロジェクトが進んでいるためか、地方団体における個人を対象にした電子署名プロジェクト事例はほぼ皆無であった。このような中、ブリティッシュ・コロンビア州政府が、土地所有権の電子登記システムを 2004 年より実用化している。

（ア）ブリティッシュ・コロンビア州土地所有権電子登記システム

ブリティッシュ・コロンビア州政府土地所有権登記局（LTB : Land Title Branch）は 2004 年より、州内の個人による土地所有権登記（譲渡、抵当、変更、放棄、納税など）申請を、電子署名を利用してオンラインで受け付けている。

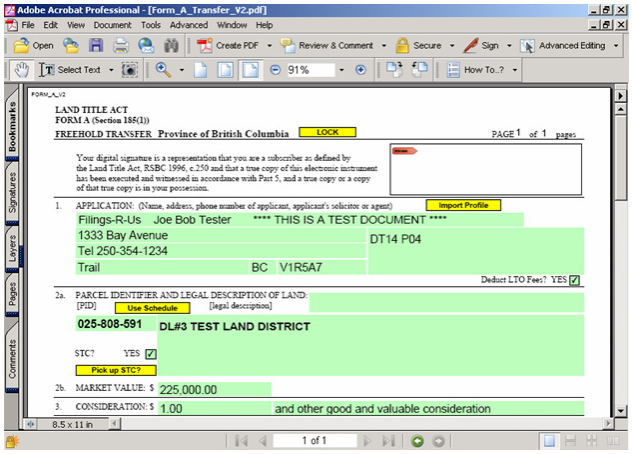
オンラインによる電子登記システムの構築にあたり、所有権登記局は、1997 年に同局の最優先課題として登記簿登録のオンライン化プロジェクトを掲げ、1998 年より電子申請委員会（Electronic Filing Committee）を新設して本格的に取り組んできた。電子申請委員会は、ブリティッシュ・コロンビア州法曹界や公証人（行政書士）、法律分野の学術会から構成され、1999 年には改正土地登記法（Land Title Amendment Act-1999、法案 93）が成立し土地所有権登記の電子申請が可能となる法基盤が整った[47]。その後、2004 年 4 月 1 日より、土地所有権登記のオンライン申請実用化が始動した。

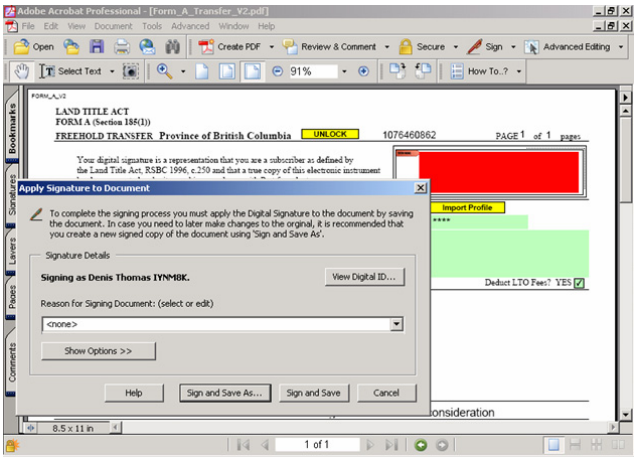
ブリティッシュ・コロンビア州における、個人を対象とした土地所有権登記の電子申請方法は、以下の手順で行われる[48]。

- 個人の PC 上に申請テンプレート（PDF ファイル）をダウンロードする。
- ダウンロードした申請テンプレートに必要事項を記入する（オフライン作業）。
- 弁護士あるいは公証人（行政書士）が電子署名を行う。
- ブリティッシュ・コロンビア州政府の電子政府機能『BC Online』経由で、登記書類を電子的に同州政府土地所有権登記局へ送信する。
- 送信と同時に、土地所有者の『BC Online』口座から土地所有料が土地所有権登記局へと引き落とされる。固定資産税の対象の場合、銀行口座から土地所有権登記局へ電子送金される。
- 利用者の電子メールに、書類番号、受領日・時間、その他送金情報などが送付される。

[47] ブリティッシュ・コロンビア州環境自然管理局。
http://srmwww.gov.bc.ca/landtitle/EFS_web_site/presentations/cle_eforms_presentation.pdf
[48] Continuing Legal Education Society of British Columbia 誌、2004 年 4 月 16 日。
http://www.cle.bc.ca/CLE/Stay+Current/Collection/2004/4/04-bcleg-efs?practiceAreaMessage=true&practiceArea=Legal%20Support%20Staff

図 1　ブリティッシュ・コロンビア州土地所有権登記局の電子申請書類と電子署名





（左：電子申請書類、右：電子署名）

出典：ブリティッシュ・コロンビア州土地所有権登記局[49]

これら電子申請サービスはすべて無料で提供される。なお、土地所有権登記登録は、書面でも引き続き受け付けている[50]。

2　公的個人認証システム

米国・カナダにおける公的個人認証システムの事例が少なかったことから、本項目では、前出のイリノイ州電子署名プロジェクト（米国）、及びカナダの公開鍵基盤『epass』を引き続き取り上げることとする。なお、両プロジェクトともに、普及状況を示す情報（ユーザ数、利用頻度などのデータ等）は公開されておらず、入手できなかった。

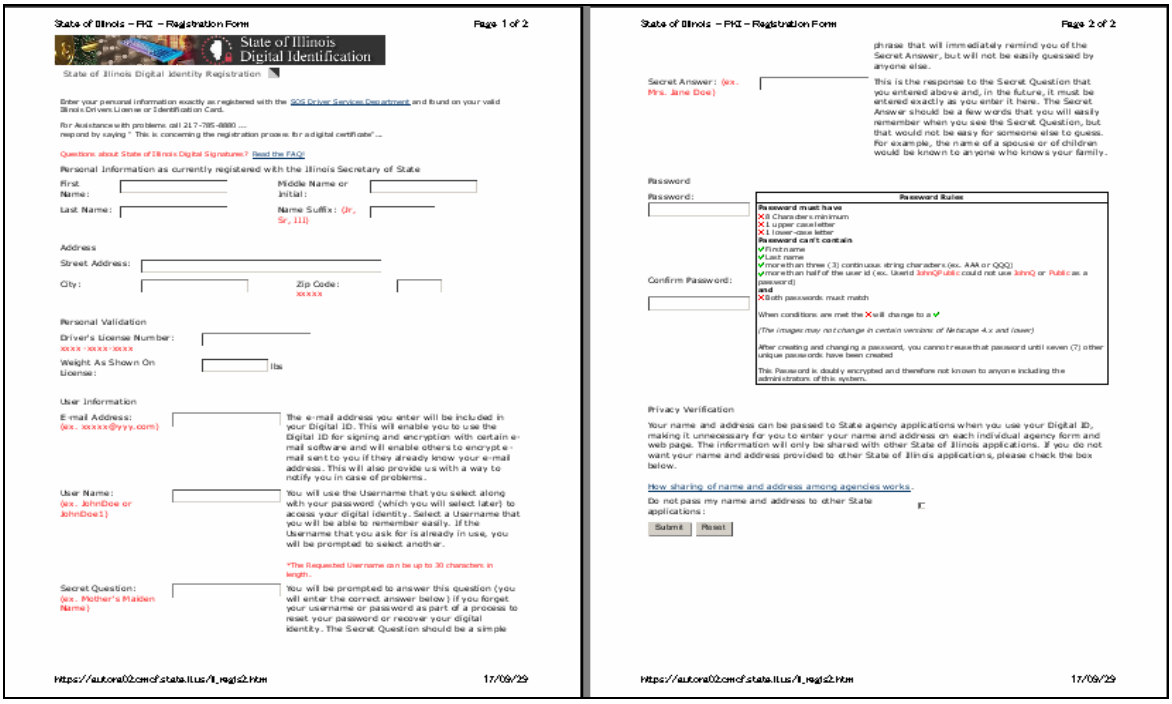
（1）個人認証システムの概要、用途、普及状況

ア．米国（イリノイ州電子署名プロジェクト）

イリノイ州の『イリノイ州政府 PKI』は、州市民が個人情報を含めた情報を一度登録すると、州政府への法的な書類も電子的に申請できる電子証明書が発行される公開鍵基盤である。現在は、医療保険などのオンライン申請を行う同州『MEDI』やオンライン納税『TAXNET』用に使用されている。電子証明書の取得には、以下表８に示す個人情報を入力する必要がある。また、登録画面は、図２に示す通りとなっている。

[49] http://www.ltsa.ca/documents/presentations/CLE_EFS_Overv_feb-20-04.ppt
[50] 法人による土地所有権登記登録は、2004 年４月１日以降、すべて電子申請へと切り替わった。

図 2　『イリノイ州政府 PKI』公開鍵基盤への登録画面



出典：イリノイ州政府 PKI ウェブサイト[51]

表 8　『イリノイ州政府 PKI』登録に必要な個人情報

必要な個人情報	追記
氏名	名（first）、ミドルネーム（middle）、姓（last）、接尾（suffix：ジュニア、二世、三世など）。
住所、郵便番号	
イリノイ州政府発行運転免許証番号	
体重	イリノイ州政府発行運転免許証に記載のあるもの。
電子メールアドレス	書類申請後の確認メールとして使用。
ユーザ ID	ログイン用に使用。
秘密の質問	ユーザ名、パスワードを失念したときに使用。 例えば「母親の旧姓」「ペットの名前」など。
上記秘密の質問への回答	
パスワード	以下の条件で構成されていること： • 最低 8 文字のアルファベットで構成 • 大文字を最低 1 文字含む • 小文字を最低 1 文字含む • 姓・名を含まない • 連続して同一文字を 3 文字使用しない（例：AAA、QQQ など） • ユーザ ID の半分以上を連続して使用しない パスワードの有効期限は一年間。 パスワードの新規作成あるいは変更後 7 日間は、別のパスワードを新たに設定することが出来ない。 また、パスワードは暗号化されるため、システム管理者へも情報は提供されない。

出典：イリノイ州政府 PKI ウェブサイト[52]

[51] https://autora02.cmcf.state.il.us/il_regis2.htm

なお、州外の市民も同様に『イリノイ州政府 PKI』を利用することができる。この場合は、イリノイ州政府が他州の運転免許証番号から個人を認証することができないため、オンラインでの登録ではなく、郵送にて申請する。この際、紙の書類[53]に必要事項を記入し、身分を証明できるものを２種類以上持参の上、公証人（行政書士）より直筆の署名を入手する。また、パスワードを失念した場合も同様、オンラインでの本人確認ではなく、直接イリノイ州政府が設置するヘルプデスクへ問い合わせる。

イ．カナダ（『epass』）

カナダ連邦政府の運営する公開鍵基盤『epass』は、カナダ連邦省庁が提供するオンライン・サービスを安全に受けるためのシステムで、このための電子証明書が市民に無料で発行される。『epass』の利用に際し、カナダ電子政府『GOL』サーバが利用者のセキュリティ・レベルをチェックし（128 ビットの暗号化を可能にするブラウザの利用を推奨）、また使用言語などの確認目的でクッキーも利用する。

『epass』は、ユーザ ID とパスワード、及び３つの復元問題及び回答を設定すれば取得できる（表９）。また、エントラスト社が提供するソフトウエアのインストールも必要となる。なお、図３は『epass』のログイン・登録開始画面である。

表 ９　『epass』取得に必要な情報

必要な情報	追記
ユーザ ID	以下の条件で構成されていること： ・ 8 文字～16 文字で構成 ・ 数字を使用する場合は最大 7 桁まで ・ 特殊記号（%、#、@など）を使用しない ユーザ ID は、設定後も変更可能。
パスワード	以下の条件で構成されていること： ・ 8 文字以上で構成 ・ 最低 1 文字以上の大文字を使用 ・ 1 文字以上の小文字を使用 ・ 最低 1 桁以上の数字を使用 ユーザ ID はパスワードとして使用できない。 また、特殊記号も使用できない。 パスワードは、設定後も変更可能。
復元問題	ユーザ ID あるいはパスワードを失念した際に利用する。 以下 3 つの復元問題と回答を設定： 1. 既に設定されている復元問題から一つを選択（新婚旅行先、初めて所有した車、最初の勤務先、子供時代の親友、初恋の相手、好きな先生、カナダの好きな場所、北米以外の旅行先、好きな教科、ペットの名前、最初のコンサート、など） 2. 思い出深い人の名前とそのヒントを設定 3. 重要なビジネスモデルとそのヒントを設定

出典：『epass』登録画面[54]

[52] https://autora02.cmcf.state.il.us/il_regis2.htm
[53] https://autora03.cmcf.state.il.us/enroll/forms/oos_app.pdf
[54] https://cmrsw005.egs-seg.gc.ca/Self-Administration_Server_1/SASFrameset_e.jsp?visibleFrameURL=https://cmrsw005.egs-seg.gc.ca/epass_app_server/epass?1128095387598

図 3　『epass』ログイン・登録開始画面

出典：カナダ政府（Government of Canada）ウェブサイト[55]

『epass』は、各連邦省庁と個人がやり取りするすべての書類（納税、年金、保険、事業登録書類など）のオンライン・サービスに必要な、ログイン作業の一部として利用される。例えば、カナダ歳入庁（CRA：Canada Revenue Agency）のオンライン納税サービス『My Account』を利用する場合、『epass』に併せ、カナダ歳入庁への登録も必要となる。この場合、社会保障番号、生年月日、納税額、郵便番号を提供して得る有効コード（Activation Code）を入力して登録する。従って、『epass』のみではカナダ連邦政府のオンライン・サービスは利用できない。

個人が複数の『epass』を持つこともできる。例えば、前出のカナダ歳入庁の『My Account』と、カナダ行政管理教育推進機構（CCMD：Canadian Centre for Management Development）の運営するカナダ公共行政大学院（Canada School of Public Service）のオンライン授業とを利用する場合、ひとつの『epass』を利用するか、あるいは別々の『epass』を作成して利用することができる。なお、『epass』は本人の利用が前提となっており、従って家族であっても第三者が代わりに『epass』を利用することは禁じられている[56]。

『epass』は、１年間のうちに最低１回以上アクセスしないと、自動的に無効となる。

[55] https://blrscr3.egs-seg.gc.ca/TruePassApp/TruePassFrameset_e.jsp?visibleFrameURL=/gol-ged/gov/AuthenticateUserInputRoamingEPF_e.html

[56] 『epass』登録時の契約内容に「本人のみが利用する」ことが含まれており、利用者はこれに同意して『epass』を取得する。

３　公的認証システムの課題と政策の方向性及び今後の見通し

米国とカナダにおける公的認証システムの課題や今後の見通しは、大きく異なっている。連邦レベルでの統一した電子認証システムおろか、省庁間での相互認証システムの動きも遅々として進まない米国は、現在も政府組織自体の慣例や IT ベンダーからの圧力といった課題を抱えている。一方のカナダは、その洗練された電子政府への取り組みが高く評価されており、今後もその完成度を増すことが期待される。

（１）米国

米国連邦政府における公的認証システムの課題のひとつが、相互認証システムの進捗の遅れがある。これは、従来、米国政府が市民の個人情報を一元管理してこなかったという情報管理体制に端を発する。例えば、納税情報についても、連邦税と州税は、それぞれ内国歳入庁（IRS）と州政府の納税局が個別に対応している。また、運転免許証や医師免許、弁護士免許といった各種免状については、連邦政府の介入はなく、すべて州政府レベルでの発行・管理体制が取られている[57]。更に、連邦政府省庁においても、各組織間での横の繋がりも乏しい。このような中、政府関連書類の電子化を義務付ける 1998 年政府書類削減法（GPEA：Government Paper Elimination Act）の施行の後押しなどをうけ、各省庁がそれぞれ独自に電子認証システムを構築してきた。

このような分散的な情報管理体制を是正すべく、総務庁が主体となって 2003 年より進めてきた連邦省庁間での相互認証を推進するイニシアチブ、『E-Authentication』（P 18「１　公的個人認証サービスの現状」参照）であるが、現時点では導入段階にあり各種フレームワークや技術標準の作成を目指している状態で、実際の運営には至っていない。総務庁は 2005 年４月、既存のシステムを用いて技術試験を行うべくシステム・ベンダーに対して技術提供を求めており[58]、この試験に基づいた認定ベンダー・リストを発表するに留まっている。このように、イニシアチブ発足後２年間が経過してもまだ運用の目処がつかない背景として、計画に青写真が用意されていなかった点や、技術標準作成から始める必要があったこと、2004 年 11 月の大統領選挙期間に重なり選挙中は連邦政府省庁の足並みを揃えることが難しかったこと[59]などが指摘されている。

（２）カナダ

カナダ政府の電子政府イニシアチブ『GOL：Government On-Line』は、大手コンサルティング企業のアクセンチュア社（Accenture）が実施する世界 22 カ国の電子政府評価において、その成熟度（maturity scores）で１位に選出されるなど[60]、顧客サービスを含めた高い精度が評価されている。このような中カナダ政府は、次の電子政府戦略計画として『次世代の公共サービス（Next Generation Public Services）』を掲げ、シングル・サインオンの更なる効率化や、ワンストップ・インターネットアクセスなど、利用者

[57] なお、郡や市町村における各種免状の取扱い体制は、各州政府の法規定により異なる。
[58] Government Computer News 紙、2005 年４月７日。http://www.gcn.com/vol1_no1/daily-updates/35480-1.html
[59] Network World 紙、2001 年 10 月 11 日。
[60] http://www.accenture.com/xdoc/ca/locations/canada/insights/studies/leadership_cust.pdf

の高い利便性を目指している。カナダ政府の個人認証システム『epass』は既に高い完成度を誇るものの、更なる効率化を目指す同政府は、今後も引き続き参加省庁数の拡大などを目指していくものと考えられる。

第３節　個人情報保護・情報セキュリティ対策

１　個人情報保護制度

米国における個人情報保護は、「個人情報保護法（Privacy Act）」と「情報自由アクセス法（Freedom of Information Act、以下 FOIA）」の２法、カナダにおいては、「プライバシー法（Privacy Act）」と「個人情報保護及び電子文書法（Personal Information Protection and Electronic Documents Act、以下 PIPEDA）」の２法によって大枠が規定されている。さらに、両国とも州レベルにおいても個人情報保護やオンライン情報保護、アクセスを規定する諸法律が制定されており、個人情報保護を巡る法的枠組みは非常に複雑なものとなっている。

（１）個人情報保護に関する連邦法・州法

ア．米国

ここでは、連邦単位で個人情報保護を規定する「個人情報保護法」「情報自由アクセス法」さらには、その他分野別の情報保護法について纏めた後、地方団体の例として、カリフォルニア州における個人情報保護規定を紹介している。

（ア）連邦政府

米国には日本の「個人情報保護法」にあたる政府、民間、一般市民全般を網羅する個人情報保護法は存在しない。1974 年に制定された米国連邦法の「個人情報保護法」[61]は、米国の連邦省庁が一般市民の個人情報の収集や取り扱いをする際に遵守しなければならない法律であり、民間企業や民間組織における個人情報保護を定めた法律ではない。

一方、「情報自由アクセス法」[62]は、政府が管理する情報（個人情報含む）への一般市民アクセスを保証する法律であり、個人情報保護法と一対となって情報ポリシーの基盤となっている。2002 年の電子政府法制定以来、連邦・州・地方レベルで急ピッチにオンライン化が進む米国でも、政府機関が個人情報を円滑に効率よく取り扱うと同時に、いかに個人情報を保護し、政府による個人情報取り扱いについて一般市民からの信頼を保持するかというのは大きな課題になっている。

---

[61] 連邦法典５編 552 条（a） 1974 年制定
http://straylight.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html
[62] 連邦法典５編 552 条 1966 年制定　URL 同上。

ａ．個人情報保護法（Privacy Act of 1974）」

米国における個人情報保護の法制化は、ウォーターゲート事件がきっかけとなって、連邦捜査当局などによる個人への違法な監視や操作を禁止することを目的に 1970 年代に進んだ。1974 年に制定された「個人情報保護法」の概略は以下の通りである[63]。

・米国市民は、国家安全保障や犯罪捜査などに関する一部の例外を除き、行政府機関が保管する個人情報を閲覧また複写することを保証されている。
・米国市民は、行政府機関が保管する個人情報がその他の政府のどの組織、団体、機関に保管されているかを知る権利がある。
・米国市民は、個人情報中の誤謬、欠如、不正確さなどを削除、訂正または加筆する権利がある。
・米国市民は、政府が非合法に個人情報へのアクセスを許可するなどの違法行為を犯した場合、政府を訴える権利がある。
・米国政府は、官報（Federal Registry）を通じて、どのようなファイルに個人情報が収集されているかを公開する義務がある。
・米国政府は、情報収集の当初の目的以外で情報を使用することはできない。
・米国政府は郵送によって個人情報開示依頼が提出された場合、例外案件を除きこれを拒否することはできない。
・米国行政府機関は個人情報管理官を設け、長官が該当省庁内で管理される個人情報の最終責任を負わなければならない。

さらに同法は行政管理予算局（OMB）を連邦政府における個人情報保護の総監督機関とし、次のような役割を負わせている。

・同法の履行状況の実際について監督と支援
・政府省庁が同法を履行する際のガイドラインを作成

行政管理予算局が発表しているガイドライン（M-99-05）[64]によれば、各連邦省庁は次の６活動を通じて、個人情報保護法を遵守しなければならないことになっている。

・シニアレベルの個人情報ポリシー担当官の任命
・個人情報保護法準拠の記録システムの管理・維持
・個人情報保護法準拠の記録システムが、正確で最新の完全な情報システムであることを一般通知
・秘密の個人情報記録を保管しない
・州政府、地方自治体などとの個人情報交換のシステム見直し
・個人情報保護に関連する業務結果を行政管理予算局に報告

電子政府促進の元、連邦政府における個人情報へのアクセスが一層頻繁になってきたこともあり、2002 年、政府行政責任局（GAO：Government Accountability

[63] 司法省 www.usdoj.gov/04foia/04_7_1.htm
[64] http://www.whitehouse.gov/omb/memoranda/m99-05-b.html

Office）は、政府の個人情報保護の対応状況を把握するために集中調査を行った。翌年2003 年の６月に議会に提出された報告書「個人情報保護には行政管理予算局のリーダシップが必要（OMB Leadership Needed to Improve Agency Compliance）」[65]によれば、各省庁の個人情報保護法の準拠状況は決して満足できるものではなく、行政管理予算局はより強力なリーダシップを取り、政府の個人情報保護改善に努力すべきであると提言している。

ｂ．「情報自由アクセス法（FOIA）」

米国の連邦レベルにおける個人情報保護体制を知る上で、「情報自由アクセス法（FOIA）」なしには全貌をつかむことはできない。1966 年に成立した「情報自由アクセス法」は、「個人情報保護法」より歴史が古く、一般個人の連邦行政機関の保管する情報・記録へのアクセスを保証するものである。「情報自由アクセス法」の目的は民主社会の基本的機能の一つである情報開示の確立を目指すもので、米国の「開かれた政府の真髄」[66]ともいえる機能である。賢明に予算が使用されているか、政府による違法行為がないか、個人や企業、政府関連情報の機密保持などが正しく行われているかなど、政府行政機関の有効性、効率性を検証する法律といえる。

「情報自由アクセス法」の概要は以下の通りである[67]。

・行政府の保管する記録、情報は基本的に何人にも開示されなければならない。
・行政府は省内機構、機能、規則、職員のマニュアルなどの一般情報に関しては、個別の依頼がなくても定期的に開示して、各ホームページの「リーディングルーム」と呼ぶ一般公開ページに掲載する。
・行政府は、文書による開示依頼を受領後、20 日以内（週末祭日を除く）に記録が開示可能であるかどうかを返答しなければならない。
・行政府は国家機密や犯罪捜査に関連するなどの一部の例外を除き、開示依頼を拒否することはできない。拒否する場合はその旨文書で返答しなければならない。
・情報開示依頼者は開示拒否をされた情報に対して、上訴請求をする権利を認められている。
・情報、記録の開示は複写費などを除いて無料で行われなければならない。
・行政府は毎年度末（９月末）から４ヶ月以内に「情報自由アクセス法」関連の報告書をまとめ、これを司法省に提出する。司法省はこれを、ホームページなどを通じて一般開示できるようにし、最終的には議会に提出する。

ここで繰り返しになるが、「情報自由アクセス法」はあくまで連邦省庁の情報に関する法規で、州や地方自治体の保管する情報については、各州、各自治体がそれぞれの州法や条例を制定して対応しているので「情報自由アクセス法」は適用されない。連邦省庁には同法をまとめて管轄する中央機関は存在せず、各省庁が自省の記録や情

[65] GAO-03-304 http://www.gao.gov/new.items/d03304.pdf
[66] ジャネット・レノ前司法長官 www.usdoj.gov/oip/intorduc.htm
[67] 司法省 www.usdoj.gov/04foia/referenceguidemay99.htm

報の管理、開示を行っている。ただし、行政機関へのガイダンスや「情報自由アクセス法」関連の質問受付、職員への「情報自由アクセス法」訓練など政府内の統一機能は、司法省の情報プライバシー局（Office of Information and Privacy）が果たしている。

ｃ．「連邦情報セキュリティ管理法（FISMA）」・「米国愛国法（Patriot Act）」

2002 年に電子政府法の一部として成立した「連邦情報セキュリティ管理法（FISMA：Federal Information Security Management Act）」、また、同時多発テロ事件以降に制定された 2002 年の「米国愛国法（USA Patriot Act）」は、国家安全保障に関わる連邦機関の情報及び資産の安全のための全国的で包括的な枠組みを定めた法律である。

「連邦情報セキュリティ管理法」は適用対象が政府機関のみならず、民間請負業者や関連業者で取り扱われる情報や情報システムも含まれるので、連邦政府だけにしか適用されない「個人情報保護法」よりさらに適用範囲が拡大されているといえる。また、テロリスト防止を前面に可決された「米国愛国法」も、従来に比べて連邦捜査局などによる犯人の電話盗聴や個人情報の検索規制を緩和しており、公的機関の個人情報へのアクセスがしやすくなった。

この結果、炭素菌事件関連で容疑者に間違えられた一般市民が、連邦政府捜査局を訴える事件や、航空会社の一般乗客がテロリスト容疑者と誤って搭乗を拒否されるケースなど、政府機関による一連の個人情報侵害が多発した。こうした傾向に対して人権擁護団体の米国市民自由団体（American Civil Liberties Union）や電子プライバシー情報センター（Electronic Privacy Information Center）などから、「政府が、犯罪やテロの可能性の薄い一般市民の個人情報にまでアクセスを許されるのは、権力の乱用だ」との強い懸念の声が上がっている。

ｄ．分野別の情報保護法

連邦レベルの法律には全般的な個人情報保護法はないが、代わりに分野別個人情報保護を規制する法律が多数存在しており、主なものは以下**表 1** の通りとなっている。

表 1　個人情報保護に関する諸法

分野	法律名（英文名）	内容	制定
運転免許	自動車登録運転免許個人情報保護法（Driver's Privacy Protection Act）[68]	各州や自治体の交通運輸局が管理する運転免許関連の個人情報を保護する。	1994 年制定（連邦法典 18 編 2 第 721 条）
電子通信	電子通信個人情報保護法（Electronic Communication Privacy Act）[69]	連邦政府機関による「有線傍受規制法」の範囲を拡大改正したもので、電子メール、無線、携帯電話、その他コンピュータを使用しての通信傍受全般を規制し個人情報を保護する。	1986 年制定（連邦法典 18 編第 2510 条-2522 条、2701 条-2711 条、3121 条、1367 条）

[68] http://straylight.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002721----000-.html
[69] http://straylight.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_119.html

分野	法律名（英文名）	内容	制定
教育	家族教育の権利と個人情報保護法（Family Educational Rights and Privacy Act）[70]	連邦省庁や政府から補助金を受けている教育機関による個人情報の漏洩を規制して個人情報を保護する。	1974 年制定（連邦法典 20 編第 1232 条（g）
金融	公正信用報告保護法（Fair Credit Reporting Act（FCRA））[71]	消費者の個人情報を管理する連邦省庁、信用照会担当機関などに対して、情報報告の公正性と正確性を義務付けし、消費者の個人情報を保護する。	連邦法典 15 編第 1681 条-1681 条（u）
金融	負債公正取立て法（Fair Debt Collection Practices Act）[72]	金融取立て業者が、不正に個人情報を利用して負債取立てをすることができないように、消費者を保護する。	連邦法典 15 編第 1692 条[73]
金融	金融サービス近代化法（グラム・リーチ・ブライリープライバシー法）（Financial Services Modernization Act, Gramm-Leach-Bliley （GLB）, Privacy Rule）[74]	金融機関が消費者の個人情報を収集する際、消費者に対する適切な通知を義務付け、外部金融機関に対しては消費者が個人情報流用拒否の選択を持つことを保証する。	1999 年制定　連邦法典 15 編第 6801 条-6809 条
消費者一般	ビデオ個人情報法（Video Privacy Protection Act）[75]	ビデオ売買や賃貸の際の個人情報を保護する。	1998 年制定　連邦法典 18 編第 2710 条
医療	医療保険携帯責任法[76]（Health Insurance Portability and Accountability Act（HIPAA））[77]	医療保険関連情報の電子化を促進し、さらに個人情報を保護する。	1996 年制定
消費者一般	連邦個人情報窃盗横領抑止法（Federal Identity Theft Assumption and Deterrence Act）[78]	個人情報窃盗犯罪を連邦レベルの犯罪に格上げする。	1998 年制定　連邦法典 18 編第 1028 条
児童	児童オンライン個人情報保護法（Children's Online Privacy Protection Act（COPPA））[79]	未成年のオンラインにおける個人情報を保護する。	連邦法典 15 編第 6501 条
政府	コンピュータ詐欺乱用防止法（Computer Fraud and Abuse Act）[80]	許可なく政府省庁や州間業務に従事する金融機関などの「プロテクトされた」コンピュータの内容を改ざん変更することを禁じる。	1984 年及び 1986 年制定　連邦法典 18 編第 1030 条

[70] http://straylight.law.cornell.edu/uscode/html/uscode20/usc_sec_20_00001232---g000-.html
[71] http://www.ftc.gov/privacy/privacyinitiatives/credit.html
[72] —
[73] http://straylight.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00001692----000-.htmlhttp://straylight.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00001692----000-.html
http://www.ftc.gov/privacy/glbact/glbsub1.htm[74]
[75] http://straylight.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002710----000-.html
[76] US Department of Health and Human Services http://www.hhs.gov/ocr/hipaa
[77] http://aspe.hhs.gov/admnsimp/bannerps.htm#privacy
[78] http://straylight.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html
[79] www.ftc.gov/ogc/coppa1.htm
[80] http://straylight.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html

分野	法律名（英文名）	内容	制定
政府	コンピュータ検索個人情報保護法（Computer Matching & Privacy Protection Act）[81]	連邦政府省庁間、州政府間などで個人情報が取り扱われる際の規制を強め、個人情報を保護する。	1974 年の個人情報保護法の一部修正法（1988 年、1990 年）　連邦法典 5 編　第 552 条（a）

出典　カリフォルニア州連邦プライバシー法ウェブサイト[82]

ｅ．審議中の連邦法案

現在連邦レベルで審議中の個人情報保護内容を含む新法案、改正法案[83]は、上下院あわせて 50 にも及んでおり、その注目の高さが伺われる。以下はその一部の法案例である。

・電子メールプライバシー法（E-Mail privacy Act of 2005）
・ワイヤレスプライバシー法 （Wireless Privacy Protection Act of 2005）
・学生プライバシー保護法（Student Privacy protection Act of 2005）
・消費者プライバシー保護法（Consumer privacy Protection Act of 2005）
・アメリカ安全ウェブ法（U.S. Safe WEB Act of 2005）
・社会保障オンライン保護法（Social Security On-line Privacy Protection Act）
・図書館、書籍、個人記録保護法（Library, Bookseller, and Personal Records Privacy Act）
・個人情報窃盗防止法（Identity Theft prevention Act of 2005）
・金融個人情報保護法（Financial privacy Protection Act of 2005）
・テロ防止・アメリカ保護法（Protecting America in the War on Terror Act of 2005）
・機密情報認可法（Intelligence Authorization Act for Fiscal Year 2006）

（イ）地方団体の情報保護政策―カリフォルニア州の例

カリフォルニア州では、2000 年には州法[84]で消費者省（Department of Consumer Affairs）内に個人情報保護課（California Office of Privacy Protection）[85]が設置され、州民の個人情報の保護、消費者のプライバシー保護啓蒙活動を、英語とスペイン語の２ヶ国語で開始するなど、個人情報保護政策の整備に力を入れている。カリフォルニア州政府が実施する情報保護政策の具体例[86]は以下の通りである。

[81] www.4law.cornell.edu/uscode/html/uscode18
[82] http://www.privacy.ca.gov/lawenforcement/lawspv.htm
[83] http://thomas.loc.gov/cgi-bin/query/bdquery において、「Privacy Act」で検索した結果。
[84] California Business and Professions Code Sections 350-352A
[85] http://www.privacy.ca.gov
[86] http://www.privacy.ca.gov/lawenforcement/laws.htm

ａ．個人情報一般

・情報手続法（Information Practices Act of 1977、加州民法 1798 条）：州政府の行政部門による個人情報収集、管理、開示などに関する制限を規定[87]。

・情報共有開示法（Information-Sharing Disclosure、加州民法 1798.82-1798.84 条）：通称「シャイン・ザ・ライト法（Shine the Light）」。一般企業が保管する顧客の個人情報に対する情報開示を規定[88]。

・オンライン個人情報保護法（Online Privacy Protection Act of 2003、加州商法 22575-22579 条）：消費者から個人情報を収集する全ての商業サイトに、個人情報保護方針を明確に提示することを義務付ける[89]。

ｂ．分野別情報保護法

＜クレジットカード関連＞

・消費者信用照会代理業法（Consumer Credit Reporting Agencies Act、加州民法 1785.1-1785.36 条）：連邦「公正信用報告保護法」の州法版で、消費者信用照会業務全般を規定する。信用照会代理業社は、①個人情報窃盗被害者や、クレジット発行会社からクレジットカード発行拒否を受けた消費者に無料で信用照会を提供する、②個人情報窃盗の結果を信用照会に掲載しない、こと等が定められている。

・クレジットカード情報開示規制法（Credit Card Full Disclosure Act、加州民法 1748.10-1748.12 条）：クレジットカード会社が顧客の個人情報を第３者に開示する際は文書をもって通知し、顧客は開示を拒否する権利を有する。

＜自動車・運転免許関連＞

・自動車「ブラックボックス」法（Automobile “Black Boxes” Vehicle Code 第 9951 条）：自動車製造業者に対し、2004 年 7 月 1 日以降に製造された車両に航空機のブラックボックスにあたる「車両データレコーダー（エンジン機能、速度、ブレーキなどをセンサーで記録）」を装備するよう規定。

・運転免許証情報機密法（Driver’s License Information Confidentiality-Vehicle Code、自動車法第 1808-1821 条）：州運輸局が当事者の許可なく個人の自動車免許内容を開示することを禁止。

・運転免許証情報スキャン又はスワイプ法（Driver’s License Information, Scanning or “Swiping”、民法第 1798.90.1 条）：飲酒業などが消費者の年齢を運転免許証によって確認したり、自動車販売業者が顧客の自動車運転免許内容を記録したりする際、元々の目的以外で個人情報を流用することを禁止。

[87] http://www.privacy.ca.gov/code/ipa.htm
[88] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84
[89] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579

ｃ．個人情報窃盗防止対策例

以下はカリフォルニア州が州民に提唱している個人情報窃盗防止対策例である。

・各個人の社会保障番号の保護を推奨。銀行や信用照会または政府の一部と偽って電話、電子メール、郵便などで個人情報を聞いてくるフィッシングと呼ばれる詐欺行為に注意する。
・銀行の月末清算書やクレジットカードの請求書情報などをむやみにゴミ箱に捨てない。また、毎月の清算書などをきちんと照合する。
・金融機関は個人情報をその個人の許可なしで他の会社などに流用してはならない。また個人情報を銀行などが同列の企業間などで使用しないように要求する拒否権（opt-out）も保障する。
・Pre-approved（信用照会済み）のクレジットカードを極力利用しない。発行機関には個人情報などが記載されたクレジットカード勧誘のダイレクトメールなどの郵送中止を要請する。

このような注意を行っていても個人情報窃盗にあってしまった州民に対しては、被害者登録制度システムを設けて対応している。このシステムでは、個人情報を盗まれて被害にあった州民が、州司法省が管轄する「被害者届け登録簿（Identity Theft Registry）」に登録することで、他人が使ったクレジットカード被害額については責任を負わなくてもよいとするものであり、法の保護を受けることができることになる。この被害者リストへの登録は、オンライン＜http://caaag.state.ca.us/idtheft/general.htm＞で行うことができ、さらには、無実申し立ての方法や裁判所からの証明書の取り方なども示されている。その他にも、無料電話相談も設けられている。

また、実質的に国民背番号のような機能を果たす社会保障番号についても、カリフォルニア州では、個人情報保護の立場からその開示を抑える方向に動いている。同州の州条例（州民法条例 1798.85）では、2004 年以降、社会保障番号の保護対策が以下のように取り決められている[90]。

・ID カードやバッジなどに社会保障番号を明示しない。
・郵送物には社会保障番号を明示しない。葉書など外から見えるものにも社会保障番号を明示しない。
・インターネットではパスワードのしっかりしたもの、「安全なサイト」と明示されたものなど以外には社会保障番号を提示しないなど、提示、使用には細心の注意を払う。
・個人は一般企業に対して、個人の社会保障番号を顧客番号として使用しないようにという依頼をする権利を有する

[90] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.85-1798.86

イ．カナダ

ここでは、連邦規模で適用される個人情報保護法２つについて紹介した後、オンタリオ州における個人情報保護法の例を取り上げている。

（ア）連邦政府

カナダにおける個人情報保護は「プライバシー法（Privacy Act）」と「個人情報保護及び電子文書法（PIPEDA）」 の２つの連邦法によって全般的基準が定められている。プライバシー法は連邦政府における個人情報保護に、PIPEDA は官民全般の IT 媒体の個人情報保護に適用される。連邦政府における個人情報には、中央連邦政府下の政府機関と、政府の全国的規制に遵守しなければならない銀行・鉄道・放送・電話・航空会社などが保管・維持をする個人情報も含まれる。

ａ．「プライバシー法（Privacy Act）」の概要

1983 年に成立したカナダの「プライバシー法」は、個人情報の収集、訂正、開示、保管、また使用に関する条項を網羅している。同法によると、カナダ国民は情報を取り扱う政府行政機関に対して、情報の閲覧、開示、アクセスを要求する権利をもち、政府はこれに対して個人情報を正確に取り扱うための制度を確立する義務がある。また、カナダ総督会議（Governor in Council）によって任命された個人情報監督官（Privacy Commissioner of Canada）が、政府からは独立したオンブズマンとして個人情報に関する争議、苦情などを収集、調査、解決する権限を持つ。カナダの「プライバシー法」の概要は以下の通りである 。

・カナダ国民の個人情報とは、氏名、生年月日、住所、電話番号、ID 番号、指紋、血液型、婚姻の有無など、また、人種、宗教、教育、医療、犯罪、雇用、金融などの情報、政府と取り交わされた文書、特定の個人に対する他の個人の意見などを含むものとする。
・カナダ国民は連邦政府が保管、維持、使用する個人の情報の開示を要求する権利を有する。カナダ国民は連邦政府が管理する個人情報保管機関（一般に個人情報バンクと呼ばれる）へのアクセスを保証されている。
・カナダ国民は連邦政府における個人の情報の加筆、削除、訂正などの権利を有する。
・カナダ国民は過去２年まで遡って、連邦政府が使用した個人情報の目的先を明確にするよう要求することができる。
・カナダ国民は連邦政府が使用した個人情報の目的また個人情報の開示拒否などに対して、文書を持って苦情を訴えることができる。
・カナダ連邦政府は個人情報開示の要求が提出された場合、30 日以内に返答する義務がある。開示拒否をする場合には、その旨正式に依頼者に返答しなければならない。
・カナダ連邦政府はカナダの公用語である英仏二ヶ国語のどちらかで返答しなければならない。

・カナダ連邦政府は以下のような場合に限って、個人情報開示の拒否をすることができる。
  ⅰ） 外国政府や国際機関に関連する個人情報
  ⅱ） 犯罪捜査や犯罪防止関連に関する個人情報
  ⅲ） 州政府が保管維持する個人情報
  ⅳ） 要求者以外の個人に関する個人情報
  ⅴ） 個人の医療情報（情報開示がその個人に対して悪影響を与えると認められる特定の例外を除く）
・個人情報監督官は個人情報に関する苦情を受領後、これを調査する権限を有する。また、毎年度末後３ヶ月以内にカナダ国会に調査報告書を提出する義務を負う。

ｂ．「個人情報保護及び電子文書法（PIPEDA）」

カナダの「個人情報保護及び電子文書法（PIPEDA：Personal Information Protection and Electronic Documents Act）」は、2000 年の立法化以来、隔年毎に改正を続けて、現在まだ成長過程にある新しい法律といえる。コンピュータやインターネットの普及によって、官民ともに電子媒体による個人情報や一般文書の管理維持量が莫大に増えたが、1983 年成立の「プライバシー法」では電子化時代における個人情報保護がうまく対応できないという懸念が積もるようになった。さらに、政府管理の個人情報だけでなく、民間が商業活動をする際に収集、維持、管理をする個人情報についても、規制が必要になってきたため、同法の制定に至ったという経緯がある。

当初「個人情報保護及び電子文書法」の適用対象は、連邦政府機関の請負をする請負業者、また州間にわたって業務を取り扱う鉄道、航空、テレコム、銀行、放送業などの民間組織に限られていたものの、2002 年の同法改定において、これらの企業、団体、商業組織の職員の医療、保険に関する個人情報も「個人情報保護及び電子文書法」 の対象に含むようになった。さらに、2004 年１月からは、カナダ国内で個人情報を取り扱う官民企業全般に適用されることになり（但し、各州政府機関や、単一州内のみで商業活動を行う州政府の請負業者など一部は対象外）、包括的に個人情報保護を規定する法律となった。

「個人情報保護及び電子文書法」の概要は以下の通りである 。
・顧客の個人情報を収集、使用、開示する際には、顧客の同意を必要とする（一部策定中の法案や政府の機密情報などの例外を除く。）
・個人情報を使用できるのは顧客が同意した目的のみに限られる。
・顧客からの同意があった場合でも、個人情報の使用は一般に適当と認められた案件に限られる。
・顧客は商業活動によって収集、使用される個人の情報を確認変更する権利を持つ。
・連邦政府の個人情報監督官は、同法（および上記プライバシー法両法）の元、個人の権利が尊重され個人情報の侵害が行われていないかを監督する。また、同法に関連する苦情を受領し、これを調査報告する義務がある。

（イ）州レベル

カナダ国内の州・準州は基本的に連邦法に準拠するが、各州で独自の州法が制定されている場合もある。例えば、ケベック州は「民間における個人情報保護法（Act Respecting Protection of Personal Information in the Private Sector）」[91]を制定しており、カナダ連邦政府はその準独立性を認めている。また、アルバータ州[92]とブリティッシュ・コロンビア州[93]２州でも、それぞれ連邦法に準拠する「個人情報保護法（PIPA : Personal Information Protection Act）」を制定しているため、重複を避けるために州法の規定が優先されている。その他の州、または州間での情報関連、商業活動全般では上記連邦法が現在のところ直接適用されるが、カナダ国内のいくつかの州では「個人情報保護及び電子文書法」に準ずる独自の州法を検討中である。

また、州レベルでも連邦政府と同じような個人情報監督官が任命されているか、あるいはまたオンブズマンのシステムを利用して監督が行われている。

以下ではオンタリオ州における個人情報保護法制定状況について簡単にまとめている。

ａ．オンタリオ州における個人情報保護法

オンタリオ州では、州政府・地方自治体が収集・管理している個人情報保護は、1988 年制定の「情報の自由・プライバシー保護法（Freedom of Information and Protection of Privacy Act）」と 1991 年制定の「自治体情報の自由・プライバシー保護法（Municipal Freedom of Information and Protection of Privacy Act）」の２法によって規定されている[94]。２法の内容は基本的には同じだが、前者は州政府の各部局、委員会、州立大学などが対象、後者は市役所、公立学校、厚生局、公共事業、消防署、警察署など地方自治体が対象と、規定対象者が異なっているのが特徴である。

同２法の概要は以下の通りである。

- オンタリオ州民は、州政府また地方自治体やその他機関によって収集・保管・利用・開示・処分される個人情報に自由にアクセスする権利を有する。
  オンタリオ州民は政府機関に対して個人情報の開示を依頼する際、５ドルの費用を支払う。
- オンタリオ州民は政府機関に対して個人情報の内容を修正する際、10 ドルの費用を支払う。
- 政府局間の機密情報、第３者に関する機密情報、依頼者以外の第３者の個人情報などは公開しない。また、立法化以前の法案草案や非公開会議の記録、局内使用の提言内容、警察捜査内容、経済的損害を発生しうる情報なども情報公開の例外とする。

---

91 http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html

92 http://www.psp.gov.ab.ca/index.cfm?page=legislation/act/index.html

93 http://www.legis.gov.bc.ca/37th4th/3rd_read/gov38-3.htm

94 オンタリオ州情報プライバシー監督官室　http://www.ipc.on.ca

・オンタリオ州政府は、個人情報保護に関して以下の義務を負う。

ⅰ）個人情報保護に必要な記録保管のシステムを確立する。

ⅱ）開示の依頼を受けた情報が、依頼者の個人情報か第３者の個人情報も含むものかを決定する。

ⅲ）依頼受領後 30 日以内に、当情報が開示可能なものであるかを決定しその旨通知する。

ⅳ）開示拒否の場合、その理由も通知する。

ⅴ）開示拒否の場合、依頼者はオンタリオ州情報プライバシー監督室に上訴請求する権利（請求費 10 ドル）を有することを 30 日以内に通知する。

またオンタリオ州では、オンタリオ州議会によって情報及びプライバシー監督官が任命されているが、公正な監督活動ができるよう行政府とは独立の立場が保障されている[95]。

（２）個人情報漏洩の際のポリシー

米国、カナダとも、連邦法・州法制度は整備が進んできているが、情報漏洩の際のポリシーは適応される法規によって、また漏洩の状況によって違ってくる。

ア．米国

個人情報漏洩に係る罰則は、統一された規定がなく、既述したように分野別に存在する個人情報保護法各法においてそれぞれに規定されているのが現状である。一方、州政府の代表としてここで取り上げるカリフォルニア州は、2003 年に成立した「個人情報漏洩通知法」によって個人情報漏洩の際のポリシーが統一的に規定されている、全国でも非常に珍しい地方自治体である。

（ア）連邦政府

2005 年５月に発表されたシークレットサービスとカーネギーメロン大学（Carnegie Mellon University）の共同報告「インサイダー脅威報告（Insider Threat Study）」[96]によれば、米国連邦政府内における IT システム・ネットワークへの侵入などの事件には、前職員の報復目的による情報漏洩事件が多いという。

一般に連邦政府の職員がその公的立場を悪用して、故意に個人情報の漏洩をしたり、漏洩した情報を利用しての悪用行為に及んだ場合は、「プライバシー法」の規定により 5,000 ドル以下の罰金が課せられる[97]。

しかし、米国においては分野別に個人情報保護を規定する法律が存在しているため、どのような分野の個人情報を漏洩したかによって、その罰則規定は様々となっている。例えば、医療関係の情報の場合、「医療保険携帯責任法」の定めに従って、政府職員

[95] オンタリオ州情報プライバシー監督官室　http://www.ipc.on.ca
[96] Insider Threat Security: Computer System Sabotage in Critical Infrastructure Sectors. www.secretservice.gov/ntac/its_report_050516.pdf.
[97] 米国連邦法典５編 552 条(i) Criminal penalities

に限らず一般の漏洩に対する罰金は民事の場合一件で 100 ドル（年間で２万 5,000 ドル以下の罰金）、利益を得るために故意にまたは悪意を持って個人の医療情報を売買するなどの刑事犯罪の場合だと、年間で最高 25 万ドル及び 10 年間の禁固刑となっている。その他、「公正信用報告保護法」で規定する個人情報漏洩の場合、2,500 ドル以下の罰金[98]、さらには、「コンピュータ詐欺乱用防止法」違反の場合は最高 5,000 ドル以下の罰金と、１年～20 年の懲役が罰則として課せられる[99]。

（イ）カリフォルニア州

カリフォルニア州の「シャイン・ザ・ライト法（前出）」は、一般企業が保管する顧客の個人情報に対する情報開示を規定した州法だが、民事の違反案件につき 500 ドルの罰金、故意または悪意による違反の場合、最高 3,000 ドルの罰金が課せられることになっている。

さらに、同州は、2003 年７月に連邦法・州法を通じて個人情報の漏洩を取り締まる最初の法律「個人情報漏洩通知法（Security Breach Notice Act[100]）」が制定されたことでも非常に有名である。この法律によって、カリフォルニア州市民の情報を取り扱う州政府はもちろん、州民を顧客に持つ州内外の民間企業や一般団体組織でも、個人情報が漏洩されたという疑いがある場合、顧客に通知を義務付けることが定められた。この法律はカリフォルニア州法ではあるが、インターネットや通信販売を通じてカリフォルニア州在住の顧客と商業的取引を行った企業や組織に対しても適用されるため、結果として全米規模で適用されている。同法で保護の対象とされる個人情報には、州民の氏名、住所、生年月日などの基本的なものから、社会保障番号、運転免許証の情報、クレジットカードの番号、パスワードなども含まれる。

同法は、それまで、顧客個人情報盗難事件が発生しても、企業がイメージダウンを避けるためにその事実を公表しないことが多く、さらなる被害を招いてきたという懸念の元、制定された。同法成立後、顧客情報の漏洩事件は表面化され始め、一般の消費者が漏洩による被害に対して知る権利を認識し始めるようになったといえる。「個人情報漏洩通知法」の下で、個人情報盗難事件の被害者であることが明らかとなった数は、連邦・州政府、企業、団体（大学なども含む）など全体で 5,000 万にも及んでいるという[101]。同法は消費者側からは個人情報盗難による被害を最小限に抑える役目を果たす一方で、政府・民間機関側からすると、消費者保護が手薄であるというイメージを生まないよう、より効果的な個人情報保護体制を整備するきっかけを生む法律となっている。

2005 年 11 月現在、「個人情報漏洩通知法」または類似の法律を審議している州は全米の半分に達しているが、今のところ法制化しているのはカリフォルニア州１州にとどまっている。その他、カリフォルニア州選出のダイアン・ファンステイン連邦上

[98] http://www.ftc.gov/os/statutes/fcra.com
[99] http://www.4.law.cornell.edu.uscode/html/uscode18
[100] California Civil Code 1798.29 www.leginfo.ca.gov/calaw.html
[101] カリフォルニア州サンディエゴ市の電子プライバシー情報センター（Electric Privacy Information Center、http://www.epic.org）の調査による

院議員（Diane Feinstein）の音頭取りで、現在連邦議会にも類似の連邦法案が提出されている。

イ．カナダ

カナダにおいても、複数の法律によって個人情報漏洩に関する罰則規定が定められている。

（ア）連邦

「プライバシー法」68 条では、同法に違反して、個人情報を漏洩した場合の罰金は最高で 1,000 ドルと定めている。また、「個人情報保護及び電子文書法」の場合は、個人情報を漏洩した場合、または、個人情報を漏洩したりその疑いがあることを政府監査官に知らせた内部密通者を当該企業が解職・停職などの不当な扱いを行った場合については、起訴されない場合は最高 1 万ドル、または正式に起訴される事件については最高 10 万ドルの罰金が処せられることが同法 28 条で定められている。

（イ）オンタリオ州

オンタリオ州においても、個人情報保護を取り締まる州法それぞれに、個人情報を漏洩した場合の罰則が独自に定められている。例えば、オンタリオ州の「個人医療関連情報保護法（Personal Health Information Protection Act、2004 年成立）」では、故意に他人の医療関連情報に不正にアクセス・修正・悪用した場合、カナダ国民の場合罰金最高 5,000 ドル、非カナダ国民だと罰金最高 25 万ドルが課せられるとの規定がある。

2　個人情報保護政策と実施

（1）米国

米国連邦政府レベルでは、セキュリティポリシーの統一的ガイドライン作成が進められており、2006 年春に策定完成が予定されている。その他、国土安全保障の分野では、国土安全保障省が情報セキュリティ推進の旗振り役としての役割を与えられている。また、州の例として、ここではニューヨーク州とペンシルバニア州のそれぞれについて取り上げることとする。

ア．連邦政府

（ア）セキュリティポリシーの策定状況と内容

米国では 2000 年、連邦省庁における情報管理と情報セキュリティの厳重な引き締めを規定する「連邦情報セキュリティ管理法（FISMA：Federal Information Security Management Act）」が制定され、連邦セキュリティポリシー大まかな基本をまとめた法律となっている[102]。

[102] FISMA 2004 Report to Congress, march 1, 2005
http://www.gao.gov/new.items/d04483t.pdf

まず同法では、各省長官を、「情報と情報セキュリティ管理の総括的責任者」として位置づけ、単に情報・情報セキュリティの管理者とするだけでなく、「情報・情報セキュリティが危険にさらされ問題が発生した場合に全責任を負う」統括者であると位置づけている。

また、実際の監督を実施するチーフ情報オフィサー（Chief Information Officer）のポストを設け、各長官の任命により、プログラムの作成、実施、職員の教育、定期的な情報セキュリティ制御の評価と管理報告作成など、情報・情報セキュリティ全般を担当させることを定めている。

さらに、同法では、大統領府行政管理予算局（OMB）に対して情報セキュリティの管理実施と問題点に関する進捗状況報告書を毎年各省庁が提出することを定めている。特に、各省庁は情報システムのリスクマネージメント、情報セキュリティのレベル、ポリシーや手続きをコスト面から調査・分析することが義務付けられている[103]。行政管理予算局では、これら各省庁から提出された報告書をまとめ、議会に提出して評価を仰ぐことになっている。

「連邦情報セキュリティ管理法」では規定しきれない詳細なセキュリティポリシーを、別途商務省の傘下にある国立標準技術研究所（NIST：National Institute of Standards and Technology）が策定中で、現在最終策定段階にある[104]。このセキュリティポリシー、「連邦情報プロセス基準（FIPS：Federal Information Processing Standard、Special Publication 800-53A）」と呼ばれるもので、同ポリシーは、「情報資産保護手順の基準とガイドライン」と「技術専門の必要条件事項」２部分から構成される予定である。

2006 年春までに策定完成予定のこのガイドラインでは、特に、以下の３つの分野における基準を明確にし、連邦省庁及び関連機関における「連邦情報セキュリティ管理法」遵守の手引きとなることが期待されている（草案は国立標準技術研究所ホームページで閲覧可能[105]）。

・情報と情報セキュリティ管理の最少必要条件
・コスト効率性のあるリスク・アセスメントの標準
・セキュリティ保護の目標として、マネジメント、オペレーション、テクノロジーの３層からの守秘性、完全性、情報の可用性。

（イ）所管官庁及び推進機関の具体的支援策

ここでは、前述した「連邦情報プロセス基準」の策定中心となっている国立標準技術研究所と、国土安全保障における情報セキュリティの中心的組織である国土安全保障省の２機関についてまとめる。

---

[103] http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf
[104] NIST Publication 200
http://www.nist.gov/public_affairs/releases/information_security_standard.htm
[105] http://csrc.nist.gov/publications/drafts/Draft-sp800-26Rev1.pdf

ａ．国立標準技術研究所（NIST）

すでに紹介したように、「連邦情報セキュリティ管理法」をベースとしたセキュリティポリシーである「連邦情報プロセス基準」の策定は、商務省の国立標準技術研究所が現在実施している。この中でもセキュリティポリシー策定に中心的に係っているのは、国立標準技術研究所の中の、情報技術研究所（Information Technology Laboratory）のコンピュータ・セキュリティ部（Computer Security Division）で、同部の主要業務は、連邦政府 IT システムのガイドラインと技術基準の開発である[106]。特に、①暗号コード規格開発・応用、②新情報技術のセキュリティ、③セキュリティ管理、④セキュリティ検証が同部の４大業務となっている。国立標準技術研究所が現在策定を担当しているセキュリティポリシーについては、前述を参照されたい。

ｂ．国土安全保障分野における情報セキュリティ

国土安全保障分野における情報セキュリティを担当するのは、国土安全保障省である。国土安全保障省が新設されて間もない 2003 年、大統領府は報告書「セキュアなサイバースペース確立に向けた国家戦略（National Strategy to Secure Cyberspace）」[107]をまとめ、国土安全保障分野の情報セキュリティにおける国土安全保障省の 13 の役割を以下表 2 のように明示している。

表 2　情報セキュリティにおける国土安全保障省の役割

①　サイバースペースを含む重要インフラ保護のための国家レベルの計画を策定する。
②　連邦政府、州や地方自治体、民間業界とのパートナーシップを構築し、その調整に当たる。
③　サイバー攻撃、脅威、脆弱性などに関して官民の情報交換を改善し、また円滑にする。
④　全米のサイバー事件関連の分析と警告能力を強化発展させる。
⑤　事件が起こった場合の対処法、回復計画などをとりまとめて提供する。
⑥　サイバー脅威や脆弱性を発見、評価する。
⑦　サイバー脅威や脆弱性の低減努力を支援する。
⑧　サイバーセキュリティの強化努力や研究を支援促進する。
⑨　啓蒙活動を進め、サイバーセキュリティ関連の教育を促進させる。
⑩　サイバーセキュリティ専門家の訓練や資格を育成する。
⑪　連邦、州、地方自治体のサイバーセキュリティを促進する。
⑫　国際的サイバーセキュリティを促進する。
⑬　国家安全とサイバーセキュリティとを統合させる

出典　国土安全保障省

米国土安全保障省は 2003 年６月に全米サイバーセキュリティ局（National Cyber Security Division）を設置し、24 時間体制のサイバーセキュリティ中央集権機能として活動を開始した。同局はさらに、連邦政府、州政府、地方自治体、民間企業、大学などから構成されている緊急体制チームとして、米国コンピュータ緊急体制整備チーム（Computer Emergency Readiness Team、通称 US-CERT）を立ち上げている。

[106] http://csrc.nist.gov/mission.html
[107] http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

また、2004 年電子メールを媒体にした全米で始めての「全米サイバー警戒体制（National Cyber Alert System）」プログラムを設置し、政府省庁のみならず、ビジネスや一般家庭にサイバー脅威の警報、回避方法、ベストプラクティスなどを素早く通達する手段としている。米国コンピュータ緊急体制整備チームは各州政府でセキュリティを担当する省庁と緊密に連携を取りながら、サイバーセキュリティの保護と推進に当たっている。

（ウ）情報セキュリティ監査制度

情報セキュリティ監査を連邦レベルで実施するのは、政府行政責任局（GAO：Government Accounting Office）である。GAO では、毎年各省庁から行政管理予算局に提出される報告内容や（「連邦情報セキュリティ管理法」の欄参照）、独自の調査（省庁担当者に対するインタビューや検査）などを通じて、情報セキュリティの監査活動を行っている。

GAO が 2004 年度にまとめた情報セキュリティ監査報告「情報セキュリティ～「連邦情報セキュリティ管理法」遵守にはさらなる努力が必要（Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirement、GAO-04-4387）」[108]によれば、監査対象となった 24 の連邦省庁中、情報セキュリティ管理の内容が及第点であったのは半分以下の 11 省庁に過ぎなかったという。例えば、総務庁では庁内の何人の IT スペシャリストが情報セキュリティ訓練を終了しているのか把握していなかったし、エネルギー省では昨年 1926 件の情報セキュリティ関連の問題が起きているが、正式な報告は 89 件に過ぎなかったという結果が出ている。また農務省でも情報システムの８割近くの安全度調査が終わっていないという状態であることがわかった。さらに、テロ対策が専門の国土安全省でさえ、サイバーセキュリティへの脅威を正確に察知し、脆弱部分を査定してそれを回復させるための具体的非常体制への計画はできていないという惨憺たる結果が判明している。一方で、情報セキュリティ体制がうまく整備されている省庁としては、情報漏洩には懲役最高５年、罰金 25 万ドルという厳しい独自制度を課し、情報セキュリティ訓練を職員対象に毎年実施している国勢局が挙げられている。国勢局ではこのような厳しい独自規則が功を奏して、過去 35 年間に情報漏洩事件は１度も起きていないという[109]。

政府省庁の情報セキュリティ管理がなかなか改善できない一つの理由は、各省庁の情報セキュリティの担当官であるチーフ情報オフィサー（CIO）が、既存の情報システムやネットワークについては担当外で関知なしという状況にあることからきているとGAO は分析する。また、予算の制限から、大人数を抱える巨大な省庁が、スタッフ全員の情報セキュリティ訓練に手間取っているというのが現状であるという。さらに、同報告書はリスク管理、サイバー攻撃や犯罪の緩和策、訓練、緊急対応の体制や手順

[108] GAO 報告 Gao-04-4387　http://www.gao.gov/new.items/d04483t.pdf
[109] 'Slow progress on IT security, OMB says' March, 2004. Army Times.

など、「連邦情報セキュリティ管理法」法準拠の内容はほとんどの省庁で満足とはいえない状況だと報告している。

このため GAO は、以下の５項目を情報セキュリティ（特にサイバーセキュリティ）管理部門が実施すべき重要項目として提言している。

・アクセス制御：不正アクセスを禁じ、ネットワーク、情報の使用や閲覧を正当な職員に制限する。
・システム統合：悪意に基づいたコードによる改ざんや不正な変更がなされないようシステムとデータの安全を確認する。
・コード化：情報送付や保管の際、第３者が情報を読み取れないようにコード化する。
・監査とモニタ：サイバー攻撃が起こってしまった場合、その間、また事件後の調査を担当官らが円滑にできるようにする。
・コンフィギュレーション管理と確認：担当官が各機関のホスト、ネットワークにおけるセキュリティ体制を随時調整し、セキュリティ体制が継続的に機能するようにする。

イ．州レベルにおける情報セキュリティ推進・監査

ここでは、情報セキュリティ担当推進局の例として、ニューヨーク州サイバーセキュリティ・重要インフラ調整局を取り上げ、その後、州レベルにおける情報セキュリティ監査の例として、ペンシルバニア州の例を纏める。

（ア）ニューヨーク州情報セキュリティの実施例

ニューヨーク州は同時多発テロ事件の直接被害を受けた州として、全米でもリーダーの立場をとるべく、セキュリティ全般への見直しと体制再構築を目指している。ニューヨーク州のジョージ・パタキ知事（George Pataki）は、2002 年３月に、情報セキュリティを含むサイバーセキュリティ専門のタスクフォース（Cyber Security Task Force）を立ち上げ、州をあげて迅速な危機対応・発見・防止・攻撃後の回復というサイバー攻撃守備体制を重要目標に掲げた。

さらに同年９月には、州政府内に「サイバーセキュリティ・重要インフラ調整局（Office of Cyber Security and Critical Infrastructure Coordination-CSCIC）」を設置し、エネルギー・運輸・金融・政府機関へのテロ攻撃や自然災害などの物理的セキュリティ全般への対応のみならず、情報セキュリティも担当させている。

サイバーセキュリティ・重要インフラ調整局は、連邦省庁や州省庁、ニューヨーク州内の地方自治体との連携や調整を主要業務としているが、その他にも、州民向けに「サイバーセキュリティへの注意事項」と題したパンフレットをホームページに掲載して、地域住民への情報セキュリティへの啓蒙活動も実施している[110]。パンフレットの内容は、表３に示している。

[110] Cyber Security Awareness （January 2005）
http://www.scsic.state.ny.us/security/csa.html

表 3　サイバーセキュリティ・重要インフラ調整局によるパンフレット掲載内容

ユーザ名・パスワード	• パスワードは定期的に変える。 • 以前のパスワードは使用しない。 • 一箇所で使ったパスワードをまた使わない。 • 家族にもパスワードは渡さない。 • パスワードを PC に記録しない。 • できるだけ長く、一般的にはない文字列などをパスワードに使う。
家庭用 PC のセキュリティ	• 使用し終わったコンピュータはスイッチを切るか、ロック機能をかけておく。 • モデムの自動アンサー機能は消しておく。 • 修理などを業者に頼む場合は、個人情報にかかわる機密文書などは別の場所に保管する。 • ファイアーウォールやウィルス対策のソフトウエアをインストールする。 • ウィルス対策のソフトを最低週一回は新しいバージョンにアップデートする。自動アップデート機能にしておくとよい。 • 信用できないところからのソフトウエアをコンピュータにインストールしない。
ラップトップ、携帯電話	• 小型で移動に便利であるだけに盗難にあう件数が高い。ロック、パスワード機能は必ずアクティブにしておく。 • データのバックアップをする。 • 機密内容は暗号化する。 • 飛行機や車による旅行など移動中に特に盗難に注意する。

出典　ニューヨーク州サイバーセキュリティ・重要インフラ調整局

（イ）ペンシルバニア州情報セキュリティ評価・監査の例

ペンシルバニア州政府では、情報セキュリティの評価は、州総務局（Office of Administration）の中の情報技術局（Office for Information Technology）[111]の部門のひとつであるエンタープライズ・アーキテクチャー（Enterprise Architecture）が中心となって行っている。エンタープライズ・アーキテクチャーは、情報技術局内において技術基準へのコンプライアンス、ネットワーク管理、プロダクト管理、企画などを担当する部門で、セキュリティ評価フレームワークアプローチ（Security Assessment Framework Approach）と呼ばれる情報セキュリティ評価手法に基づいて評価を実施する。具体的な評価は、表 4 で示される 10 項目について行われている[112]。

[111] http://www.oit.state.pa.us

[112]http://www.oit.state.pa.us/eashare/cwp/view.asp?a=3&Q=204732&PM=1&easharePNavCtr=|#9485

表 4　ペンシルバニア州におけるセキュリティ評価項目

評価方法	内容	必要時間	対象評価となる部署からの評価参加者
情報セキュリティ方針	セキュリティ方針と手続、情報収集体制、基本構想の内容	情報収集（2 時間インタビュー2 回）、情報調査〈4-6 時間〉	一般職員
物理的セキュリティ評価	ロック、電源、HVAC、防火など環境、物理的セキュリティの評価	現地審査（1 時間）、手続審査（1 時間）	物理的セキュリティ担当職員
内部脆弱性スキャン	内部脆弱性機能によるネットワーク評価、夜間ラップトップ管理。	64 のサブネットシステム（各 1 時間）	ネットワーク・ジャックの場所が分かる職員
外部脆弱性スキャン・侵入テスト	インターネットからのネットワーク侵入検査・テスト	7.5 時間	なし
内部侵入テスト	内部 LAN システムから機密文書への侵入テスト	各テスト 2 時間	LAN 担当職員
ワイアレスセキュリティ分析	ワイヤレスネットワークのセキュリティ評価	現地審査（1 時間）、不正ネットワーク発見の場合はネットワーク毎に 1 時間	なし
サーバー・ワークステーション・コンフィギュレーション評価	5～6 箇所のサンプルサーバー、ワークステーション・コンフィギュレーション評価	2.5 時間	サーバ担当官
ネットワク・アカウント管理手続評価	デフォルトのアカウント調査	1～2 時間	ネットワーク担当職員
セキュリティー・インフラ評価	ファイアーウォール、ウィルス対策、VLAN、リモートアクセスサーバーなどの調査評価	2 時間（うちスキャンの 1 時間を含む）	セキュリティ担当職員
ビジネス継続プラン評価	今後の調査手続評価、アップデート、修正箇所の確認	1 時間	ビジネス企画担当職員

出典　ペンシルバニア州情報テクノロジー局[113]

このようにシステム評価が情報技術局によって行われる一方、情報セキュリティ監査は、コンピュータ監査の一環として[114]州政府の予算局や監査局が実施することになるが、どの情報システムに重点化して優先的に監査を行うかは、次の 2 段階の優先対象基準に基づいて決定される。

ａ．第 1 基準

ｉ）リスク・重要性：州民サービスへのインパクトが大きく重要性の高いプロジェクト、コンピュータシステムである場合。

ⅱ）管理者からの要請：プロジェクトまたはシステム管理担当者からの監査要求依頼度が高い場合。

113
http://www.oit.state.pa.us/eashare/cwp/view.asp?a=3&Q=204732&PM=1&easharePNavCtr=|#9485

114 http://www.oa.state.pa.us/oac/lib/oac/MDs/325-6.pdf

iii）連邦法・州法への準拠：プロジェクトまたはシステム監査が関連の連邦法・州法で決められている場合。

iv）予算：プロジェクトまたはシステム監査費が監査予算全体に見合うものである場合。

b．第2基準

i）その他の機関による監査：特定のプロジェクトまたはシステム監査が他の機関（例えば、総監査局、州予算歳出委員会、第3者の公認会計事務所または公認会計士、外部のコンサルタント、プログラムのモニタなど）による監査によって、追跡監査を必要とする場合。

ii）プロジェクトの性格：不定期に行われるプロジェクトや特殊なプロジェクトの場合（非効率性やシステムエラーの度合が高い）。

iii）プロジェクトの複雑性：オペレーションの複雑性が高い場合（複雑性が増すと当然情報量も多くコントロールシステムも複雑になり監査の必要度が高まる）。

iv）プロジェクトの歴史的背景：既存プロジェクトやシステムが監査記録によって脆弱性を指摘されている場合。

v）内部のコントロール：システム内部のコントロールが脆弱でそれまでの監査に記録されている場合。

vi）予算額：プロジェクトやシステムに多額の予算がつぎ込まれている場合。

vii）監査期間：前回の監査から時間が経っている場合。

viii）予算額：予算額超過の場合。

ix）監査がプロジェクトの効率性を高めると考えられる場合。

x）人事、手続、操作、組織などに大きな変化があった場合。

xi）特定のプロジェクトの開始または終了が、州民一般へのネガティブな評価を引き起こすと見られる場合。

（2）カナダ

カナダでは、連邦政府が定める政府セキュリティポリシー中で情報セキュリティの取り扱いが定められており、連邦政府における総括的なポリシーが存在している。連邦主導の情報セキュリティが進んでいるためか、州レベルにおけるセキュリティポリシー策定・実施状況はあまり活発でないようである。

ア．連邦

（ア）セキュリティポリシーの策定状況と内容[115]

[115] なお、セキュリティに関連する法律として、カナダでは、2001年12月に情報セキュリティ法（Security of Information Act）[115]を制定し、従来の「政府機密法（Official Secret Act）」を補足する形で情報セキュリティの法体制を強化した。実際のセキュリティ管理実行に当たっては、2003年3月の「情報セキュリティ実施基準法（Operational Standard for the Security of Information Act）」が用いられていたが、2004年5月にさらに「セキュリティ基準（Management of Information Technology Security-MITS Standard）」を設定し、管理制御、リスク・アセスメント、システム内の脆弱性への対応、セキュリティ・オフィサーの役割などを明確にした

カナダでは連邦政府レベルのセキュリティポリシーである「政府セキュリティポリシーCanada Government Security Policy）」[116]を 2002 年２月に公布している。この「政府セキュリティポリシー」は、物理的と情報の両方においてセキュリティに係る事件が発生した際の緊急体制、調査、防止プランなど、連邦政府におけるセキュリティ全般を網羅した総括的なポリシーとなっている。しかし、このポリシーは、カナダ連邦政府が所有する資産及び、カナダ連邦職員に対する危機のみを取り扱う非常に対象範囲の狭いポリシーである。さらに、本ポリシーは、大まかな方向性を示すだけに終わっており、詳細な手続きやガイドラインについては、各省庁が策定することが取り決められている。

14 章から構成される「政府セキュリティポリシー」のうち、セキュリティ保護対応に関する各省庁の活動内容について規定しているのは第 10 章であるが、そのうち情報セキュリティに関する規定は 10 章 12 項「情報技術セキュリティ（Information Technology Security）」の中で以下のように定められている。

- 各省庁は、情報技術セキュリティ管理を実施する。脅威・リスク評価実施により必要とされた場合、追加でより厳しい管理手法を採用する。定期的にセキュリティ評価を実施し、第３者による独立的評価も得なければならない。
- 各省庁は、セキュリティ脅威により（ウィルス等の被害によるシステムダウンなど）、システム運用に遅れがないよう、常にシステムをモニタリングする。
- セキュリティ事件が発生した場合、効果的に事件に対応できるようなメカニズムを整備し、情報交換をタイムリーに関係者・関係機関と行う。
- 事件が発生しても主要サービスを途切れなく提供するためのプランを、各省庁が策定する。

（イ）所轄官庁および推進機関の具体的支援策

「政府セキュリティポリシー」の所轄機関となっているのは、首相と大臣６人で構成される財務委員会（Treasury Board）となっている。しかし、財務委員会事務局のもとで、実際にセキュリティ全般の政策推進を実施しているのは、カナダ国家警察（Royal Canadian Mounted Police）、カナダ情報局（Canada security Intelligence Service）、重要インフラ・緊急準備局（Office of Critical Infrastructure and Emergency Preparedness）などの各省庁である。財務委員会事務局の中で、情報セキュリティを担当しているのは、チーフ情報オフィサー局（Chief Information Officer Branch）である。チーフ情報オフィサー局では、政府内の情報システムアップグレード、情報技術セキュリティに関連する情報管理、個人情報保護と情報セキュリティに関する技術規格の認定、プロジェクト実施など情報セキュリティ全般におけ

[116] Canada Government Security Policy （Feb. 1, 2002） http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg1_e.asp#eff

る責任を負っている。特に、チーフ情報オフィサー局が実施する活動は具体的には以下の通りとなっている[117]。

- カナダ政府全体における情報セキュリティの効率性を向上させるため、業務協力・情報共有・技術協力などの協力体制構築。
- 各省庁内の情報管理向上を目指し、政府情報管理ポリシーの段階的開発と実施。
- 各省庁が実施する重要 IT プロジェクトの評価、実施状況のモニタリング。
- カナダ連邦政府の統合的業務の見直しと、業務遂行方法の定義確立、実施の監督。
- IT・人事・予算管理などの政府業務の向上を、連邦共通インフラを通じて促進・管理するプログラムの確立・実施。

さらに、各連邦省庁では、セキュリティ・オフィサー（Security Officer）を任命し、セキュリティ保護に関するプログラムの設立と実施を行っている。セキュリティ・オフィサーの責務は以下の通りとなっている。

- セキュリティに関する省内手続きの設立、訓練、資産確認、セキュリティリスク管理、共有情報と資産確認
- アクセス制限
- セキュリティ審査
- 物理的セキュリティ
- 職員安全保護
- 情報技術セキュリティ
- 非常時のセキュリティと調査

ａ．国土安全保障分野における情報セキュリティ

カナダでも米国と同じく、国土安全保障分野において情報セキュリティ保護体制が整えられている。カナダでは、2003 年 12 月に、内閣再編成を行ってアン・マクレラン副総理（Anne McLellan, Deputy Prime Minister）が大臣を兼ねる公共安全・緊急体制準備省（Minister of Public Safety and Emergency Preparedness）を設置し、国土安全保障という面からのサイバー・情報セキュリティを担当させている。

公共安全・緊急体制準備省では、サイバーセキュリティ対応の一環として、2005 年２月にカナダ・サイバーインシデント対応センター（CCIRC：Canadian Cyber Incident Response Centre）[118]を立ち上げ、サイバー攻撃の警報やアドバイスの発信、ベストプラクティス報告、テクニカルなアドバイス、攻撃後の回復方法や予防方法などを随時掲載して、サイバー攻撃やテロに備えるための 24 時間準備体制強化サイバーセキュリティの啓蒙と情報発信を実施している。

[117] http://www.tbs-sct.gc.ca/cio-dpi/about/abu-ans_e.asp?format=print
[118] http://www.psepc.gc.ca/ccirc

（ウ）情報セキュリティ監査

カナダ連邦政府省庁の情報セキュリティ監査は、カナダ監督総局（Office of the Auditor General of Canada）が実施している。監督総局は、毎年財政監査報告を国会に提出することを義務付けられているが、これとは別に情報セキュリティの監査報告を実施しており、2002 年以降、これまでに２回、情報セキュリティ関連の監査報告書を国会に提出している。

2005 年２月に発表された当局の最新の報告書（Report of the Auditor General of Canada）[119]は、2002 年の第１回報告書のフォローアップの性格を持つもので、監査総局の監査結果に加えて、財務委員会事務局のコメントも掲載されている。監査方法として、財務委員会事務局が事前に行った連邦省庁内 82 部署からのアンケート調査の内容評価、通信セキュリティ部（Communication Security Establishment）または第３者機関による技術テストの結果検討、また、各省庁の IT セキュリティ担当官からのヒアリング、セキュリティ関連の文献調査が中心に行われた。

同報告書は、監査の結果、カナダ政府の IT 情報セキュリティは、多くの分野で改善は見られるものの、まだ満足できる水準には達していないと結論付け、政府機関の大部分の IT システムが、損害を引き起こす可能性の高い情報漏洩の危機にさらされていると分析している。さらに、政府省庁のシニアレベルの間でも、依然 IT 情報セキュリティの重要性や漏洩の危機への認識が不足しており、個人情報保護が危機にさられることで国民個人が損害を被り、政府オンライン化への信頼が崩れてしまうことに対しての対策が全く不十分な状態だという厳しい査定内容が示されている。

特に報告書では、カナダ政府機関における改善が必要な情報セキュリティ分野は以下の通りとしている。

- サイバー進入の監視
- インシデント管理
- セキュリティ関連訓練
- 請負業者のセキュリティ
- 資産の確認と分類
- 攻撃・リスク管理
- 調査、制裁
- 省、局内のセキュリティプログラム
- 職員の保護
- 国外におけるセキュリティ
- 情報交換

これらの提言に対して、財務委員会事務局は全面的に合意するコメントを寄せており、カナダ連邦政府における省庁横断型の情報セキュリティ協力が必要であるとしている。

ａ．州

今回の調査においては、特に活発的に情報セキュリティポリシー策定・運用や、情報セキュリティ監査を実施している州は見られなかった。各州においては情報セキュリティを担当する担当官は存在しているものの（例えば、オンタリオ州政府では、政府事業チーフ情報オフィサー局（Office of the Corporate Chief Information

[119] Report of the Auditor General of Canada-February 2005 （2002 年に政府セキュリティポリシーが改正されてから第２番目の報告書）

Officer）が情報セキュリティも含め、電子政府、州事業戦略、企画サービスの管理を実施しているが、情報セキュリティは主要業務となっていない）、情報セキュリティ体制が構築されている州はまだ稀といえる。

3　情報安全管理の認証

（1）米国

米国では、情報安全管理の認証イニシアチブが連邦レベルで実施されている。これは、「全米情報安全パートナーシップ（NIAP：National Information Assurance Partnership）」と呼ばれるもので、国家安全保障局（NSA：National Security Agency）と国立標準技術研究所（NIST）が共同で実施している[120]。全米情報安全パートナーシップでは、国内法や国際規格に基づいて、情報安全管理分野における共通基準の設定、IT 製品の安全性評価や認可が行われている。

全米情報安全パートナーシップでは、管理システム国際規格である ISO 規格 15408 に基づいて、保護プロファイル（PP：Protection Profile）認証システムを開発している。保護プロファイル認証システムは、連邦政府による情報処理関連製品及び情報処理システムのセキュリティ・レベルを評価するためのもので、2002 年 10 月以降、保護プロファイル認証システムの基準に沿っていると認定された製品・システムは、「米国連邦政府保護プロファイル（US Government Protection Profile: USGPP）」の認証を受けることが出来る。

情報セキュリティへの攻撃侵入脅威は、技術の発展と共に一刻一刻増加しているため、一度「米国連邦政府保護プロファイル（USGPP）」の認証を受けても、永久的に安全性を保てるわけではない。したがって認証を受けた製品・システム製品は定期的に再認証を受ける必要がある。しかし認証手続は時間と経費がかかるので、全米情報安全パートナーシップでは関連業界と協力をして再認証基準に必要な期間を考慮中であり、現在は、既存の製品に技術面での改善がなされた場合については、認証猶予期間として 18 ヶ月を認めて対処している。

全米情報安全パートナーシップから認証を受けることのできる製品・システムのカテゴリーは以下の通りである[121]。

- ウィルス対策
- キー回復
- PKI/KMI
- スイッチとローター
- バイオメトリクス
- リモートアクセス
- システムアクセス制御
- マネジメント認証
- モバイルコード
- セキュリティ・マネジメント
- 可信性のある DBMS
- ガード
- ネットワークマネジメント
- 機密データ防御
- VPN
- IDS/IPS
- オペレーティングシステム
- シングルレベルウェブサーバー

[120] http://niap.nist.gov/
[121]具体的製品バージョン名は、全米情報安全パートナーシップのホームページ＜http://niap.nist.gov/cc-scheme/pp/index.html＞に詳しい。

- 安全なメッセージ
- トークン制
- ファイアーウォール
- マルチドメイン・ソリューション
- ワイアレス LAN
- 周辺スイッチ
- スマートカード

（2）カナダ

カナダ標準協議会（SCC : Standard Council of Canada）は、連邦政府の通信セキュリティ局（Communications Security Establishment）と協力して、1998 年に情報処理システムや情報セキュリティ関連製品のセキュリティ・レベルを評価・検査する認証制度を制定した。同認証制度は、政府および民間企業両方の情報セキュリティシステムの認証を目的にしたものである。同認証制度は次の項目に適用される。

・共通項目（コモン・クライテリア）製品やシステムの評価
・IT 製品の評価
・電子商取引の安全性の評価
・バイオメトリック機器の検査
・脆弱性およびセキュリティ検査
・商業用特別セキュリティ機器の検査

また 1999 年には、セキュリティシステム評価・検査を実施する組織を認定する際に利用されるガイドラインを、以下のように２つ作成している。

・情報技術セキュリティ評価・検査を行う機関の認定ガイドライン（Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities:CAN-P-1591B、2003 年２月更新）
・情報技術セキュリティ評価・検査を行う機関の審査チェックリスト（Check list for the Assessment of Information Technology Security Evaluation and Testing Facilities: CAN-P-1592）

ア．個人情報保護・情報セキュリティ対策のアウトソーシング

個人情報保護や情報セキュリティのアウトソーシングは、連邦政府、州政府、地方自治体、また民間企業を問わず、諸刃の剣とも言える性格を持つ。例えば、情報セキュリティのアウトソーシングを受注する会社は、現在ネットワーク管理、侵入危険度の評価やファイアーウォール防御の脆弱性査定までの全体的サービスを 24 時間体制で提供しており、専門性が非常に高いことから結果として質の高い IT システム管理を受けることが期待できる。また、アウトソーシングをすることで、経費や時間の節約が可能になる事もアウトソーシングが頻繁に利用される理由のひとつとなっている。

しかし、一方で、委託企業できちんと個人情報保護が行なわれているか、また、情報セキュリティが十分に実施されているかは、委託元である政府が日々監督することができず、実際の運用形態については知りうることができないという懸念がある。さらに、グローバリゼーションが進む IT の世界においては、米国・カナダの国内以外に情報やデータ

が転送されて国外で管理されることもあり、情報保護がきちんと行われるのかという懸念を生み出している。

（ア）米国

以下では、連邦政府とフロリダ州におけるアウトソーシングについてまとめている。

ａ．連邦政府の情報セキュリティ分野におけるアウトソーシング

米国では、2002 年の国土安全保障省の成立によって、連邦省庁内の安全保障関連部門が統合されたが、これに伴い各省庁の情報セキュリティ監査の専門官である監査長官（Inspector General）や IT 監査職員が大量に同省に転任することとなった。この結果、各省内で「連邦情報セキュリティ管理法（FISMA）」遵守において大きな役割を受け持っていた専門官が不足する事態が発生し、アウトソーシングに頼らなければ行政管理予算局に毎年提出すべき情報セキュリティ報告書が完成しないという現象が起こったため、これをきっかけに情報セキュリティ分野でのアウトソーシングが急速に進んだ。

例えば、司法省では税関局、シークレットサービス、連邦警察訓練センター、アルコール・煙草・銃器局の一部を国土安全保障省に移管させたが、これによって、これまで司法省に所属していた情報セキュリティ関連の職員 165 人中 62 人、IT 監査チーム 14 人中９人が国土安全保障省に異動する結果となった。毎年度末の９月末に提出が義務付けられている情報セキュリティ報告書は、各省庁のチーフ情報オフィサー（CIO）と監査長官の監督の元、情報セキュリティガイドラインに沿って情報セキュリティ担当職員が作成し、各省庁の進捗状況をまとめるという専門的な作業が必要であるが、担当職員・監査チームの多くが異動した結果、国家機密に係る情報システム以外の監査に関しては、アウトソーシングに頼らざるを得なくなったという。同省のジェフリー・ラッシュ監査長官（Jeffrey Rush, Jr.）は、今後さらに情報セキュリティ分野におけるアウトソーシングの度合いは増えていくと予測している[122]。

IT 関連のアウトソーシングが進むにつれ、インドや中国、シンガポールといった米国外のオフショア企業（または米国企業の海外拠点）へのアウトソーシングが行なわれる可能性も出てきている。一方、政府内では、外国企業や米国企業海外拠点において個人情報保護や情報セキュリティが管理されることに対する懸念も大きく、賃金の低い中国やインドへのアウトソーシングが増加するにつれて、IT 関連の国内雇用が減少していることが懸念される中、連邦政府の IT 雇用までが国外に出て行くことに対して国民や政治家が敏感になっているという分析もある[123]。オフショア企業による IT サービスを完全に遮断することが難しい中、連邦省庁では、厳しいセキュリティ条件を満たした企業に対してのみアウトソースするという措置を取ることで対応するようになっている。

[122] ‘Treasury IG will outsource FISMA reporting’ Government Computer News, Mar.16, 2004.
[123] “Offshore outsourcing draws fire from Hill” Government Computer News, Sept. 11, 2003.

なお、連邦政府における個人情報保護についてのアウトソーシングについては、今回の調査において情報は得られなかった。

ｂ．フロリダ州政府におけるアウトソーシング

州政府における電子政府化が進む中、IT インフラの整備を含む IT アウトソーシングが積極的に行われるようになった。しかし、大規模な包括的 IT アウトソーシングが行われる例は非常に少なく、小規模なアウトソーシングを複数実施するというのが州レベルでは、多く見られる。例えば、コネチカット州では、1999 年に、IT サービス・サポートインフラ整備・管理を EDS（Electronic Data Systems Corp.）に一括アウトソーシングしようと計画していたところ、州政府が要求する要件に合わないということで取りやめの要請が EDS 社から出ている。また、2002 年になってジョージア州も、18 億ドルに上る通信 IT インフラ整備に向けた一大アウトソーシングプロジェクト実施の計画を取りやめ、代わりにもっと小規模な委託プロジェクトを複数行うことを決定している[124]。

フロリダ州は、IT 業務のアウトソーシングを積極的に促進してきた州の代表例として取り上げられることが多い。ジェフ・ブッシュ州知事（Jeff Bush）は、IT 業務のアウトソーシングを進めるイニシアチブ「マイフロリダ・アライアンス（MyFlorida Alliance）」を 2002 年に立ち上げている。このイニシアチブの元、2003 年には、アクセンチュア社（Accenture）とベアリングポイント社（Bearing Point）に対し、それぞれ、ヘルプデスク整備・運営（8,700 万ドル）とデータセンターサービス整備・運営（１億 2,600 万ドル）を委託する複数年契約を結んだことが発表されたものの、2004 年になって、入札の際の不透明な選考などがスキャンダルとなり、これらのプロジェクトは実施されることなく中止に追い込まれた。

「マイフロリダ・アライアンス」はこのまま立ち消えかと思われた 2005 年２月になって、情報セキュリティのリスク評価実施を、カリフォルニア州を拠点とするダインテック社（DynTek）に約 450 万ドルで委託することが発表されている（契約期間２年、１年の追加更新可）。ダインテック社は、州政府省庁、地方自治体、州立大学などのデータシステムや情報技術インフラの情報セキュリティ評価を行う予定となっている。

ダインテック社は、情報セキュリティ業務を得意としており、フロリダ州政府以外からも、以下のような地方自治体から情報セキュリティ業務のアウトソーシングを受注している[125]。

・フロリダ州タラハシー市
・ニューヨーク州交通局
・ニューヨーク州司法局
・ニューヨーク市厚生病院局
・ミシガン州更正局

[124] “Florida to stay outsourcing course,” Washington Technology. February 23, 2004.
[125] http://www.dyntek.com/company/clients.asp

・マサチューセッツ州厚生局
・バージニア州更正局
・カリフォルニア州ハンチントンビーチ市
・ネバダ州ノース・ラスベガス市
・ネバダ州ラスベガス市
・ミシガン州ワレッドレイク学校区

なお、州レベルにおける個人情報保護に関するアウトソーシングの例は、今回の調査では入手できなかった。

（イ）カナダ

カナダについては、個人情報保護や情報セキュリティに限った例については今回の調査で入手できなかった。ただし、ブリティッシュ・コロンビア州については、医療保険プランのアウトソーシングに関して、個人情報保護に対する懸念が高まったという経緯があるため、これに関連する情報について以下にまとめる。

2004 年、ブリティッシュ・コロンビア州政府は、州政府が運営する厚生保険の医療サービスに関連する業務を米国ベンダーにアウトソースをするという計画を発表した。しかし、これに対して、雇用が国外に流出することに強く反対した同州政府職員労働組合（British Columbia Government and Services Employee's Union）は、政府を相手取って訴訟を起こすという展開になった。また、雇用流出の問題だけでなく、アウトソース先が米国企業の場合、米国企業に委託されたカナダ市民個人情報が「米国愛国法」の遵守の対象となり、国際テロ活動捜査の名目の下で、カナダ市民が知らない間に自分の個人情報が米国政府に対して開示されるなど、個人情報保護の問題に派生することが指摘されるようになった。このため、州政府によるアウトソーシング計画の発表直後から、州政府の個人情報監査局には、政府省庁内外、メディアや人権団体などからも問い合わせや質問が殺到した。

州民からの強い懸念を払拭すべく、同州の情報・プライバシー監督官は同件に関するパブリックコメントを募集し、地元州民からの意見を幅広く募った。個人情報監査局によると、寄せられた意見約 500 件[126]は、以下の 4 種類に分類できるという[127]。

・経済性や国家安全保障の名の下に個人のプライバシーの権利を侵害されることへの懸念。
・自由貿易の促進と情報技術業界のグローバリゼーションが、国家の独立性と個人のプライバシー問題に与える影響。
・情報技術の発展に伴って、政府が必要以上のデータバンク拡大を目指し、その反面個人情報保護が国家安全保障の影で二の次になってしまった。同時多発テロ事件以後の政府の個人情報開示の傾向への懸念。

[126]' BC Attempts to Regulate International Outsourcing of Personal Information' Deeth Williams Wall LLP. http:www/dww.com/articles/bcpatriot_amendments.htm
[127] 'The USA Patriot Act & Personal Privacy-Implications for Government Contracting' Cyber Security for Government Conference. Canadian Institute, Ottawa. Sept 28&29, 2005

・国家安全保障の目的のため、国境警備や運輸方面などで警察による個人情報アクセスが緩和され、州政府の従来の役割である市民の人権保護と、法の執行や警察機能の区別が不鮮明になってしまうことへの懸念。

州民からの強い懸念に反応したブリティッシュ・コロンビア州政府は、2004 年 10 月に州政府の個人情報保護法である「情報の自由及び個人情報保護法（Freedom of Information and Protection of Privacy Act : FOIPPA）」を一部改正する州条例 73 号（Bill 73）を発令し、州政府が収集・管理する個人情報に対してカナダ国外からアクセスすること、また、このような個人情報を国外で保管することを禁止・制限する措置を取っている[128]。さらに、この条例のもとでは、外国政府による情報開示要求があった場合、要求をうけた団体・企業は州政府当局に報告通知をする義務を負うことになった[129]。

イ．地方団体が参加する ISAC

（ア）米国

ここでは、米国内の組織として、州間情報共有センターと、全米州政府チーフ情報オフィサー連合の２つを取り上げている。

a．州間情報共有分析センター（MS-ISAC）

州間情報共有センター（Multi-State Information Sharing Analysis Center : MS-ISAC）は、連邦政府、州政府、また地方自治体間において、IT・ネットワーク攻撃事件情報や、情報セキュリティの安全保障に関わる情報を、即時にまた円滑に共有することを目的として、ニューヨーク州の呼びかけにより 2003 年に設立された。東部の数州で始まった州間情報共有センターは、２年半を過ぎた現在、カンザス州以外の 49 州及びコロンビア特別区が参加する全米組織に成長している。

州間情報共有センターの掲げる目標は以下の通りとなっている。

・サイバーシステム上の脅威を速やかに警告・公開する。
・業界別のセキュリティ関連の情報交換をする。
・セキュリティ計画の分析や傾向を提供する。
・効果のあったセキュリティ運用法やアドバイスを公表する。

州間情報共有センターのメンバー州は毎月の定期報告以外に、新型ウィルス情報、サイバー攻撃ニュースや警告等を、電話や電子メールを利用して、担当官同士で必要に応じて報告し合っている。また、ホームページ＜http://www.cscic.state.ny.us/msisac/＞には各州内におけるサイバーセキュリティ情報や報告書、情報セキュリティ関連のイベントなどを随時掲載して、即戦力のある有益な情報を交換しあえるようになってい

[128] www.oipcbc.org
[129] 'BC Attempts to Regulate International Outsourcing of personal Information.' Deeth Williams Wall, LLP. Nov 10, 2004 www.dww.com/articles/bcpatriot_amendments.htm

る。警告レベルをカラーコードで示すという連邦国土安全保障省の「サイバー警告」システム（National Cyber Alert System）に似たシステムを採用することも現在考慮中で、さらには、エネルギーや金融業界など民間企業が参加する ISAC である全米 ISAC 委員会（National ISAC Council）とも近い将来情報セキュリティ分野における協力体制を強化する予定となっている。

州間情報共有センターは、連邦政府国土安全保障省と共同で、2004 年６月には「全米ウェッブキャスト（National Webcast Initiative）」と名うった産官協力型イニシアチブ立ち上げている。このイニシアチブは、２ヶ月に１回、情報セキュリティに関連するプレゼンテーションをネットで一般に公開するもので、これまでに以下のようなトピックについてプレゼンテーションが行われている。

・サイバーセキュリティ（2004 年６月）
・リスクマネージメント（2004 年８月）
・サイバーセキュリティにおけるヒューマンファクター（2004 年 10 月）
・アドウエア、スパイウエア（2005 年２月）
・脆弱性管理（2005 年３月）
・ボットネット（2005 年５月）
・ワイアレスセキュリティ（2005 年７月）
・インターネットにおける児童保護（2005 年 10 月）

なお、「ウェッブキャスト」イニシアチブに協賛の民間企業は以下の通りとなっている。

- アクセンチュア
- エーオン
- AT&T
- CDW-G
- シスコシステムズ
- CMA
- コンピュータアソシエーツ
- D&D コンサルティング
- アーンスト＆ヤング
- ファンドストーン・マッカフィー
- ガートナー
- HP
- IIC
- ISS インク
- ジェイディーシステム
- キーン
- MCI
- マイクロソフト
- ノーテル
- ノベル
- NYSTEC
- オラクル
- SAIC
- SAS
- SRA インターナショナル
- サイベース
- シマンテック
- ベリタリス

ｂ．全米州政府チーフ情報オフィサー連合[130]（NASCIO）

全米州政府チーフ情報オフィサー連合は、1960 年代に全米 20 州の政府内オフィス自動化担当官が集まって設置した自動化技術・データプロセシング委員会（Committee on Automation Technology and Data Processing）が前身となる組織

[130] National Association of State Chief Information Officers www.nascio.org

で、2001 年からは、全米州政府チーフ情報オフィサー連合（National Association of State Chief Information Officers : NASCIO）と名前を改め、州政府チーフ情報オフィサーの IT ビジネス連絡役を果たしている団体である。

現在は 50 州及びコロンビア特別地区の担当者だけでなく、一部連邦政府省庁のチーフ情報オフィサーや IT 担当者も参加しており、今季はウィスコンシン州のテクノ情報局長のマット・ミゼウスキー氏（Matthew Miszewski）が連合会長を務めている。

同連合は年次定例会、州政府チーフ情報オフィサーのネットワークや、州政府 IT プロジェクトの調査・分析、出版、教育、連邦政府の IT 政策ウォッチなども行う。また、その他州政府連合である全米州政府予算管理担当官連合、全米州政府テレコム技術担当官連合、州間情報共有センターなどとも連絡をとっている。また、プライバシー委員会、情報セキュリティ委員会など委員会を 12 設置し、連邦政府のポリシーの傾向分析、ロビイング活動、出版などの幅広い分野における情報共有活動をしている。ただし、州間情報共有センターのようなサイバー警告実施を主要業務とせず、あくまで情報交換とロビイング活動をする団体である。

（イ）カナダ

カナダにおいて、サイバーセキュリティ警告サービスを提供したり、情報セキュリティ対策の情報交換を行う ISAC に関する情報は、今回の調査では得られなかった。

第２章　イギリスの事例

第１節　電子政府・自治体の概要

１　電子政府・自治体の現状

1999 年３月に英国では政府が政策報告書「政府の近代化（Modernizing Government）」を発表し、電子政府構想を打ち出した。この構想は、ICT を積極的に活用することにより、国、地方を問わず、公共サービスの質を向上すること、公共サービスへの地域住民のアクセスを容易にすること、行政コストを改善させることを推進するというものである。また、公共サービスの提供を 2002 年までに 25%、2005 年までに 50%、2008 年までに 100%を電子化するという目標が設定された。なお、2000 年３月に、目標である 100%の達成時期を 2005 年に前倒しする発表がなされた。

政策報告書「政府の近代化」中の公約を実現するため、政府は 2000 年４月に戦略文書として「電子政府～情報化時代における公共サービスのための戦略枠組み（E-government ～A strategic framework for public services in the information age）」を発表し、国民と企業のニーズに焦点を合わせた政府の戦略において、情報化時代における政府の役割、電子政府計画を進めていく上でのビジョンに関する枠組みを述べている。また、この戦略文書において、以下の４つの電子政府の指導原則が述べられている。

①全ての国民が自由に選択できるサービスの構築
②政府及び政府が提供するサービスの利便性の向上
③ソーシャル・インクルージョン（社会的包括）の促進
④情報の効果的な利用

なお、③のソーシャル・インクルージョン（社会的包括）とは、貧困者や失業者、ホームレス等社会から排除されている人々の社会的参入のことである。

一方、地方自治体に対するガイドラインとして、政府は 2000 年４月「電子政府の実現（地方自治体のためのガイドライン）（Implementing e-government (Guidelines for Local government)）」を発表した。このガイドラインは上記戦略文書で展開された地方自治体の役割、地方自治体に対する支援及び今後の取り組みについて提示したものである。

またオンライン化を目指す地方自治体を支援するため、2001 年２月に政府は「地方自治体オンラインの実現～2005 年の目標のための重要な取り組みと財源について（e-Government Delivering Local Government Online～Milestone and resources for the 2005 target）」を発表し、2001 年度のパスファインダー（草分け的）事業に名乗りをあげる地方自治体を募集した。パスファインダー自治体は、国家的事業の開発および優秀な実践（ベストプラクティス）事例の普及を行い、政府、他の地方自治体、地方自治体協議会（LGA）、英国改善開発庁（I&DeA）と協力した取り組みを行うものである。

さらに、イングランドの全地方自治体は 2001 年以降、2005 年までの電子サービス供給のビジョンと計画を含む「電子政府実現声明書（'Implementing Electronic Government'(IEG) statement）」を作成し副首相府（ODPM）に提出することを求められ、副首相府は必要条件を満たす声明書を提出した地方自治体に対して助成を行っている。

このように政府や地方自治体は 2005 年末までに 100%の公共サービスを電子的に利用可能とする目標の実現に向けて取り組んでいる。政府レベルでは、2004 年末に内閣府の電子政府ユニット（Cabinet Office, e-Government Unit）が、2004 年 12 月現在で政府の 75%のサービスがオンライン利用可能な状態となっており、2005 年末には 96%に達する見込みであると発表している。一方、地方自治体レベルでは、2005 年８月に副首相府の電子自治体担当大臣が 2005 年３月現在でイングランドの地方自治体の 77%のサービスがオンライン利用可能な状態（2002 年３月現在では 26%）となっており、2005 年末の 100%達成に向け順調に進んでいることを発表している。

２　電子政府・自治体の推進体制

以下の表は電子政府・自治体の推進体制である。

	電子政府	電子自治体
政策・戦略策定機関	内閣府（電子政府ユニット） CIO カウンシル	副首相府
連絡調整機関	電子政府ユニット	副首相府
実施機関	電子政府ユニット 各省庁および政府関連機関	各地方自治体
支援機関	電子政府ユニット 政府通商局	副首相府 電子政府ユニット 改善開発庁 情報科学技術経営者協会 地方自治体協議会 地方自治体事務総長・上級管理者協会

（１）電子政府

ア．内閣府（Cabinet Office）

内閣府は英国における電子政府の政策・戦略分野を担当しており、また内閣府内には電子政府ユニット（eGU: e-Government Unit）という部局が設置されている。この電子政府ユニットが実質的に IT 政策・戦略の立案、各省庁内の電子政府担当部局との調整・支援を行っている。また、電子政府総合ポータルである Direct.gov.uk や電子認証インフラである政府ゲートウェイ(Government Gateway)も担当している。なお、電子政府担当大臣（Minister for e-government）として内閣府に閣外大臣が任命されている。

イ．CIO カウンシル（CIO Council）

2005 年１月に設置された組織であり、政府、地方自治体、警察、国民健康保険等の公的機関を代表する 30 の情報戦略統括役員（Chief Information Officer）から構成されている。CIO カウンシルは、年３回の会議を開催し、電子政府ユニットと連携を図り 2005

年以降の新たな IT 戦略を提案していくという役割を担っている。また、同カウンシルは公的部門における CIO の役割を促進し、政府 IT プロジェクトの改善を目標としている。

ウ．政府通商局（OGC: Office of Government Commerce）

政府通商局は財務省の一組織であり、政府やその他の公共部門が調達と経済活動において金額に見合う価値を達成するための支援を行うという役割を担っている。特に政府系機関に対して IT 対応の事業改革の支援のための情報提供と指導を行っている。

（2）電子自治体（イングランドの場合）

ア．副首相府（ODPM: Office of the Deputy Prime Minister）

副首相府は英国における地方自治を所管する重要な機関であり、政府と地方自治体の関係の管理という役割を担っている。地方自治体オンラインサービス開発に対する助成やパスファインダー事業など電子自治体事業全般を担当している。なお、電子自治体担当大臣（Minister for local e-government）として副首相府内に閣外大臣が任命されている。

また副首相府は、地方自治体オンラインプログラム委員会の議長を務め、電子自治体の取り組みの調整を担当している。この地方自治体オンラインプログラム委員会の構成機関は以下のとおりである。

- 電子政府ユニット（eGU）
- 政府通商局（OGC）
- 改善開発庁（I&DeA）
- 情報科学技術経営協会（SOCITM）
- 地方自治体事務総長・上級管理者協会（SOLACE）

イ．地方自治体（Local Council）

イングランドの全地方自治体は 2001 年以降、2005 年までの電子サービス供給のビジョンと計画を含む「電子政府実現声明書（'Implementing Electronic Government'(IEG) statement)」を副首相府（ODPM）に作成し提出することを求められ、副首相府は必要条件を満たす声明書を提出した地方自治体に対して助成を行っている。また、副首相府は 2004 年 4 月に各地方自治体の電子自治体の進捗状況等に焦点を当て、それに応じた補助金を配分するという「電子自治体に向けての優先度（Priority Outcomes for local e-government)」を発表している。

ウ．改善開発庁（I&DeA: Improvement and Development Agency）

改善開発庁は地方自治体の提供する行政サービス全般の効果的かつ効率的な向上を目的として、1999 年に設立された地方自治体による地方自治体のための機関であり、電子自治体の推進における主要な分野の改善開発を支援している。改善開発庁は、電子自治体を含む地方自治体の提供するサービスの先進的事例を他の地方自治体に紹介するなど情報の共有化を図り、また一連の国家プロジェクトにおいて電子自治体を支援するための必要なインフラストラクチャーを構築している。

エ．情報科学技術経営者協会（SOITM: Society of Information Technology Management）

情報科学技術経営者協会は公共部門の ICT マネージャーのための専門職協会であり、550 の異なった機関から 1,450 名以上のメンバーが加入している。メンバーは主に地方自治体に所属している専門家が多いが、警察、消防、公共住宅機関及び公共サービスの提供関連機関に所属している専門家も加入している。情報科学技術経営者協会は ICT の先進的事例等の促進、活用、開発のためのフォーラムを開催しており、また地方自治体に対して ICT および電子自治体に関する研究、助言、ガイダンスを行う重要な機関となっている。

オ．地方自治体協議会（LGA: Local Government Association）

地方自治体協議会はイングランド･ウェールズの全地方自治体を代表する機関であり、地方自治体が地域住民に対し迅速で高品質なサービスを提供していくことを支援している。また、地方自治体の声を集約し、政府に伝える役割を担っている。

カ．地方自治体事務総長・上級管理者協会（SOLACE: Society of Local Authority Chief Executive and Senior Managers）

地方自治体事務総長・上級管理者協会は英国の地方自治体の事務総長および上級管理者のための代表組織である。

3　電子政府基盤

電子政府のネットワーク基盤として、政府安全イントラネット（GSI: Government Secure Intranet）がある。政府安全イントラネットは、政府の各省庁及び各政府系機関を接続する基本的なネットワークインフラとして 1998 年 4 月にスタートしており、2004 年 2 月に改良が行われアップグレードされた。この政府安全イントラネットはインターネットを通じたコミュニティ内におけるウェブへのアクセス、電子文書交換、検索機能、ディレクトリーサービス、ウェブパブリッシング、電子メールの交換システムを安全かつ信頼できるものとしている。アップグレードにより、IP 仮想プライベート・ネットワークを基礎として、音声と画像データの転送、特定のユーザーグループのための個別の仮想プライベート・ネットワークが可能となった。また、最近では政府の各省庁及び各政府系機関という当初の境界を越えて、地方自治体もカバーするものとなっており、政府及び地方自治体において 350,000 のユーザーがこのネットワークに接続している。改良された政府安全イントラネットは電子政府において全国的な中核インフラとなることを目指している。

また、電子政府の総合ポータルサイトとして、Direct.gov.uk がある。この Direct.gov.uk はオンライン公共サービスの単一窓口であり、2004 年 3 月にスタートした。主な公共サービスの分野別（健康、教育、雇用等）及び利用対象者のグループ別（両親、障害者、若者等）に構成されており、ユーザーが他のサイトを検索する必要がないように工夫されている。また、2004 年 4 月よりデジタル TV を通じてサービスが利用できるようになった。さらに、企業、事業主に対し政府の情報やサービスにアクセスできることを目的とした個別の電子政府ポータルである BusinessLink.gov.uk が 2003 年 11 月にスタートしている。

第２節　電子認証サービス

１　法制度の概要

（１）2000 年電子通信法（Electronic Communications Act 2000）

公共部門、民間部門双方の電子商取引および電子署名等の法的枠組みを構築することによって電子通信分野における信頼性を確保することを目的とした法律であり、一部の条項を除き 2000 年５月に施行された。なお、この法律により貿易産業大臣が電子認証に関する登録業者の管理・維持を行うこととなった。

（２）2002 年電子署名（認証）に関する規則（Electronic Signatures Regulations 2002）

2000 年電子通信法及び EU 規則の実施規則であり、2002 年３月に施行された。

（３）EU 規則（The Electronic Signature Directive 1999/93/EC）

電子取引のためのEU共通のセーフガードを導入する規則であり、2001年７月に施行された。EU規則においての電子署名（認証）の定義は当該規則２条１項によると、電子媒体で提出されたデータ、またはその電子データに関連して認証手続きを経てもたらされるデータとなっている。当該規則は認証手続きを経たすべての申請に対して適応し、その契約や署名について保護するものである。また、以下の内容が盛り込まれている。

・電子署名（認証）の法的認識のための統一基準の導入と電子筆跡の法的認識の促進
・高度な電子認証資格を発行するサービスプロバイダーの統一基準の整備（サービスプロバイダーの認証）
・電子署名（認証）デバイスのセキュリティのための統一用件の整備（高度な電子署名（認証）デバイスの整備）
・署名照合のセキュリティのための提言
・EU加盟国に対し、サービスプロバイダーを認証するための任意ライセンス体制を構築することへの許可
・EU委員会に対して助言する権限を持つ電子署名（認証）委員会の設立

２　電子認証サービスの推進体制

（１）所管官庁・推進機関

ア．貿易産業省（DTI: Department of Trade and Industry）

貿易産業省は電子認証に関する法律の所管官庁であり、電子認証に関する登録業者の管理等の権限は貿易産業大臣にある。

イ．政府情報本部局電子通信セキュリティグループ（GCHQ, CESG: Government Communications Headquarters, Communications Electronic Security Group）

政府情報本部局電子通信セキュリティグループは、情報のセキュリティや中央省庁・政府系機関に対する信用情報共有を促進し、また外務省や国防省及び諜報機関と密接な関係にある機関である。

ウ．内閣府情報保証支援局（Cabinet Office, Central Sponsor for Information Assurance

(CSIA))

内閣府情報保証支援局は英国全体における情報保証のための戦略指針を提供する役割を担っている。

エ．内閣府電子政府ユニット（Cabinet Office, e-Government Unit (eGU)）

内閣府電子政府ユニットは電子政府・自治体における IT 政策・戦略の立案、各省庁内の電子政府担当部局との調整・支援を行っているほか、政府及び民間部門の IT セキュリティに関する全ての政策についても担当している。電子認証インフラである政府ゲートウェイは当該機関の担当である。

（２）サービス提供機関

ア．英国規格協会（BSI: British Standards Institution）

英国規格協会は、貿易産業省に代わって世界的な先進事例の調査を行うとともにユーザー管理組織を所管している。政府の各省庁及び各政府系機関を接続するネットワークインフラである政府安全イントラネット（GSI: Government Secure Intranet）は同協会によって規定された規格を採用している。また、地方自治体等が政府安全イントラネットに接続するためには同協会のセキュリティマネジメント規格を取得する必要がある。

イ．t - スキーム（t-scheme）

t - スキームは産業界主導の電子信用業務の認定等を管理する独立したボランタリーコンソーシアム（共同企業体）であり、電子認証を行う事業者の認定等を行っている。なお、t - スキームに対して政府は関与していない。

ウ．英国認定機関（UKAS: United Kingdom Accreditation Services）

英国認定機関は EU 規則によって設立された信用業務を認定する機関である。

３　電子認証インフラ

電子政府ユニットは、2001 年２月に電子認証インフラである政府ゲートウェイ（Government Gateway）を立ち上げた。政府ゲートウェイはインターネット上で行われる政府の電子サービスの処理において、安全な認証を可能にする中核的な登録認証システムである。ユーザーはオンラインによる政府サービスを利用するため、また政府の各省庁と継続的かつ安全な処理を行うために政府ゲートウェイに登録する必要がある。オープンスタンダードで構築されている政府ゲートウェイは、異なる省庁の異なるシステムのゲートウェイとの通信、また相互の通信を可能にすることにより、各省庁のサービスを接続して提供することを可能にしている。

ユーザーの識別方法は、政府の電子サービスの処理に応じて異なっている。t - スキームによって電子認証を行う事業者として認定された認証機関が発行した電子証明書がユーザーの識別に必要な場合と、政府ゲートウェイによって提供されたユーザーID とパスワード（ユーザーが選択する）が必要な場合とがある。後者は電子証明書によるセキュリティのレベルが低い場合である。

電子認証を行う事業者として認定された認証機関の発行する電子証明書は、組織に対して発行されるのと同様に個人に対しても発行されることとなるが、実際には組織間の商取引等のビジネス分野で運用されており、長期的には、電子政府サービスの処理における個人の認証方法として電子身分証明書の方がより望ましいと考えられている。

4　ID カード（電子身分証明書）について

英国においては出生届、死亡届、婚姻届は存在するものの、日本のような住民登録制度が存在しないため、地方自治体等の公共団体は、住民から提供される現住所を示す書類（銀行口座情報や電気・ガス・水道等の公共料金請求書等）を本人確認の拠り所にすることとなる。これはパスポートや運転免許証の発行についても同様である。また、公共料金請求書は、金融機関等での本人確認に必要とされている。

このような状況の中、不法入国者問題、テロ脅威の高まり及び個人情報流失による詐欺事件等によって、政府は英国にも ID カード（電子身分証明書）導入を法制化しようとしており、現在、国会において ID カード法案（ID Cards Bill）の議論がなされているところである。2005 年 5 月の総選挙に勝利した与党労働党のマニフェストに ID カードを導入するとの公約が明記されていたため、その導入が労働党政権の政治的な義務となっている。この ID カードは生体認証や電子署名等の個人情報を格納するマイクロチップを搭載したものであり、2008 年の導入を目指している。なお、ID カードの所持が義務付けられる対象者は英国民（16 歳以上）及び英国に 3 ヶ月以上居住する外国籍居住者となる見込みである。

一方、電子認証サービスの所管官庁である貿易産業省は、ID カードはあくまで本人確認を容易にするためのものであり、公的サービスの受給、または公的サービスの情報を得るためのものではないと理解しているとコメントしている。しかし、今後 ID カードが導入されれば、地方自治体レベルでも、行政サービス提供の際に ID カードを使用する必要性がでてくるとともに、実務レベルにおいても多くの関連機関に波及効果をもたらすことが予想される。

第３節　個人情報保護制度

1　所管官庁及び推進機関

（1）憲法事項省（DCA: Department of Constitutional Affairs）

憲法事項省は、法廷の運営や裁判制度の改善に関すること、人権や情報に関する権利、選挙運営に関する法律と政策等について担当している。英国の個人情報保護に関する法律であるデータ保護法（Data Protection Act）の所管官庁であり、データ保護、情報の公開、公文書に関する政府の政策を担っている。また、英国の情報公開に関する法律である情報自由化法（Freedom Information Act）の所管官庁でもある。

（2）情報コミッショナー（IC: Information Commissioner）

情報コミッショナーは、政府から独立した情報保護監督機関として、データ保護法の

執行・推進、データ管理者の登録管理等を担当している。情報コミッショナーはデータ保護法の下で、データ管理者に対し、データ保護法が遵守されているかどうかを判断するために必要な情報を提供するよう要求（情報通知）することができ、また違法行為を行ったデータ管理者に対して、同法遵守のため特別措置を講ずることや処理を停止させることを要求（強制通知）することができる。また、データ保護法に関連した情報自由化法の執行、推進も担当している。

2　個人情報保護制度の概要

英国では個人情報保護に関する法律として、1984 年データ保護法（Data Protection Act 1984）が制定されていたが、1995 年 10 月の EU 指令 95/46/EC（個人データの処理および当該データの自由な移動における個人の保護に関する指令）が採択され、EU 加盟国はこの EU 指令に適合するように国内法を整備しなくてはならなくなった。英国ではこの EU 指令を受けて、1984 年法を全面的に改正し、1998 年データ保護法（Data Protection Act 1998）を制定した。この 1998 年データ保護法は 2000 年 3 月から施行されている。なお、1998 年法の制定に伴い 1984 年法は廃止された。

この 1998 年データ保護法は、主要な欧州諸国の個人情報保護に関する法律と同様、官民双方を包括的に適用の対象としている。同法は「個人の権利」と「合理的な理由により個人情報を使用することの利益」を両立させるため、保有されている個人情報に関して、個人に一定の権利を与えるものである。同法では、「データ管理者（data controller）」である組織・法人に対するデータ保護原則の遵守義務、政府から独立した情報保護監督機関である情報コミッショナー（Information Commissioner）に対しデータ管理者としての登録義務等を課している。なお、同法では個人情報の主体を「データ主体（data subject）」と定義している。

データ保護 8 原則は以下のとおりとなる。

1. 個人データは公正かつ合法的に処理されなければならない
2. 個人データは明確かつ合法的な目的に沿って処理されなければならない
3. 個人データは目的に関連したものでなければならない
4. 個人データは正確かつ最新のものでなければならない
5. 個人データを必要以上に長く保持してはならない
6. 個人データは個人の権利に従って処理されなければならない
7. 個人データのセキュリティを確保しなければならない
8. 個人データの欧州経済地域外への移転は、当該国が個人情報保護について適切な措置を講じている場合に限る

上記原則は、個人データの処理に関して一般的な基準を定めている。原則 1 では公正かつ合法的な処理という一般要件を課しているが、その処理のための具体的な要件も定められている。以下の処理条件の 1 つ以上を満たさなくてはならない。

・個人（データ主体）の同意を得ている
・個人（データ主体）との契約を成立または履行するために必要である
・処理が法的義務の下で要求されている
・個人（データ主体）の重要な利益を保護するために必要である
・公務遂行に必要である（例：司法行政、裁判権）
・処理はデータ管理者または第三者の合理的な利益の達成のために必要である（個人の利益を不当に害することがない限りにおいて）

さらに極秘データ（Sensitive data）の処理に関しては、いくつかの追加条件がある。同法での極秘データとは個人の健康、人種、宗教、政治的意見、前科の詳細、労働組合員であるかどうか等のデータを指す。

また、データ保護法は保有されている個人情報に関して、個人に一定の権利を与えるものであるが、同法の下で保障されている権利については以下のとおりである。

①個人データ（データ主体）にアクセスする権利

どのような情報がコンピューターや冊子に記録保存されているかについて知ることを可能にする。

②個人情報の処理を防止する権利

本人またはその他の者に不当な損害・苦痛を与える個人情報を処理しないようデータ管理者に対し要求することができる。

③ダイレクト・マーケティングのための情報の処理を防止する権利

個人に関連する情報をダイレクト・マーケティング目的で処理しないようデータ管理者に対し要求することができる。

④人的関与が排除された機械的な決定に関する権利

個人は人的関与のない自動化（機械化）された手段によってなされた決定に対し異議申し立てをする権利がある。

⑤損害補償を求める権利

違法行為によって損害・苦痛を被った場合、個人はデータ管理者に対して損害補償を要求することができる。単に苦痛を受けた場合の損害補償については、限られた事情のみ要求することができる。

⑥データの修正、阻止（保護）、消去、破棄に関する権利

個人は、本人の情報に不正確な箇所または誤った情報についての表現が含まれている場合、データ管理者に対して個人情報の修正、阻止（保護）、消去、破棄を要求するため裁判所に申請することができる。

⑦情報コミッショナーに対し法律違反かどうかの査定を要求する権利

データ保護法が遵守されないまま個人情報が処理されたと思われる場合、情報コミッショナーに対し査定（判断）を要求することができる。もし、その事柄が法律違反と判断され、非公式的に（口頭で）解決できない場合は、問題となっているデータ管理者に対し執行通知が送付されることとなる。

データ保護法の下での違法行為については、通知違反、調達販売違反等がある。通知違反とは、情報コミッショナーに対して届出を行わなければならないデータ管理者が届出を怠ったまま個人データの処理を行っている場合や個人データを改ざんして処理した場合である。調達販売違反とは、データ管理者の同意なしに意図的または不当に個人情報を入手、公開（漏洩）する場合である。しかし、個人情報を入手、公開することが、犯罪防止・捜査のために必要である場合などは例外が設けられている。なお、ある者が個人情報を不法に入手し、その個人情報を提供または販売することは違法となる。

また、2003 年プライバシーと電子通信に関する指令（Privacy and Electronic Communications（EC Directive）Regulations 2003）が、2003 年 12 月に施行された。これは未承諾電子マーケティング（迷惑メール等）を含めた電子通信についての規則である。この規則によれば、電子マーケティングにおいて、電子メールやテキスト・メッセージなどの電子的な手段を利用することで、ビジネスの既存の顧客ではない個人に対してマーケティングを行う場合には、個人の事前の同意が必要となる。従って、将来的にマーケティングを行う予定である場合には、予め本人から明確な同意を得ることが重要となる。

第４節　地方自治体における IC カード導入の事例
―サウサンプトン・シティ・カウンシル―

１　スマートカード事業の概要

サウサンプトン・シティ・カウンシルはイングランド南部に位置する人口約 22 万人の地方自治体であり、「スマート・シティーズ（Smart Cities）」と呼ばれるスマートカード（Smart Cards）事業に取り組んでいる先進的な地方自治体のひとつである。この事業は公共サービス分野での多機能型スマートカードの利用範囲の拡大を目指すものであり、EU から 22 億ポンドの資金を受けている。またサウサンプトン・シティ・カウンシルでは事業遂行のためコンソーシアム（バス・鉄道の交通運営機関、地元産業界等から形成される共同企業体）を組織しており、交通省（Department for Transport）がその支援を行っている。

この事業は市内居住者、勤務者、さらには市内の教育機関で学ぶ者の全ての者に対して、公共部門や民間部門によって提供される多様なサービスを、多機能型スマートカードを通じて利用可能とすることが目的である。そのためには、マルチアプリケーション管理体制を開発し、ユーザーが動的にアプリケーションの加除をすることを可能にしていくことが必要となる。またスマート・シティーズ事業には、スマートカードや関連するカードの管理経路から集積された複数のデータを活用し、より技術的かつ実用的にするという更なる目的がある。

スマートカードは約３万枚発行されており、市民カード（Citizen card）とサウサンプトン大学カード（Southampton University card）の２種類がある。市民カードは交通機関、市立図書館、各種レジャー施設で利用可能であり、サウサンプトン大学カードは交通機関、大学の各種施設で利用可能となっている。

スマート・シティーズ事業のモジュールの１つは、異なるアプリケーションからのデータを横断的に分析可能にするインフォメーション・アナリシス・サービス・プロバイダー（情報分析サービスプロバイダー）によるデータウェアハウスの構築と関連している。それぞれのスマートカードにはユーザーを認識するため、それぞれのサービスアプリケーションによって使用される独自の識別子が存在する。取引情報がデータウェアハウスに送信される時には、独自の識別子は一方通行となり、かつ暗号化される。これは識別子が暗号化されることにより、取引情報を手がかりにデータウェアハウス内のいかなるスマートカードユーザーの個人情報を引き出すことができないことを意味する。スマート・シティーズ事業では、たとえデータウェアハウス内の情報が暗号化した匿名のもの（個人を特定する情報ではないもの）であっても、その情報がその他のデータベースの情報と照合することにより、個人を特定することが可能であるため、個人データとして取り扱われる（考慮される）こととなる。よって、スマート・シティーズ事業のデータウェアハウスサービスプロバイダーは、データ保護法においてデータ処理者（data processor）と位置付けられ、データ管理者（data controller）という立場のスマート・シティーズ事業のパートナーとともに、法律を遵守するための特別な条件が要求されている。

２　プライバシーに関する問題

サウサンプトン・シティ・カウンシルでは、スマート・シティーズ事業の遂行において住民の信頼が必要不可欠であることを早くから認識し、また ID カードのスキームを支援する政府系関連団体や政府による住民意識の調査をチェックすることにより、プライバシーに関する問題意識の高まりを敏感に察知していた。プライバシー問題に関しては、スマート・シティーズ事業の発端当初からの大きな論点であった。カードスキームの管理には個人情報の取り扱いが含まれるため､英国や EU のデータ保護法の遵守が要求されている。

英国の個人情報保護法である 1998 年データ保護法（Data Protection Act 1998）は、データ主体（個人データの主体である個人）に対して、一定の権利を与えるものであり、またデータ管理者（data controller）に対し、管理するデータの使用目的を明らかにさせること、また第３節２で述べたデータ保護８原則の遵守を要求している。さらに個人情報を取り扱う機関はデータ保護法の監督機関である情報コミッショナーに対し、個人情報を取り扱う旨を届け出なくてはならないため、サウサンプトン・シティ・カウンシルは情報コミッショナーに対し、個人情報の管理・処理する目的の届け出を行っている。また届け出以外の目的での個人情報を管理・処理することは違法となる。

スマート・シティーズ事業におけるスマートカードは、全ての者が読める１枚の紙ベースのようなものではなく、情報が暗号化され、さらにその情報はカード保有者のみが認識できる PIN 番号によって保護されているため､このスマートカードは個人情報を安全かつ効果的に移動する手段（方法）を提供しているといえる。

また情報コミッショナーによって開発されたシステムである「Information Padlock（情報保護のための南京錠)」をスマート・シティーズ事業に活用している。この「Information Padlock」というシステムは特定の目的において個人情報として処理されるために集めら

れたデータを利用する場合、その使用をデータ主体である個人に対し通知するというシステムである。データ管理者は、このシステムを利用することにより、「Information Padlock」の表記マークを申込書や関連する出版物、ウェブサイト等に表示することができる。これにより、データ主体である個人（スマートカードの申込者）は「Information Padlock」システムの利用を選択することが可能となっている。

なお、データ保護法のもとでは、極秘データ（人の健康、人種、宗教、政治的意見、前科の詳細、労働組合員であるかどうか等の情報が含まれる。）の処理については、さらに厳しい条件が課せられており、また極秘データに関する問題を避けるため、サウサンプトン・シティ・カウンシルでは個人の極秘データをスマートカードの情報として意図的に収集していない。

【参考文献、資料】

・英国統計局（ONS: Office for National Statistics）のサイト
http://www.statistics.gov.uk/default.asp
・「英国の電子自治体」（財）自治体国際化協会（2003 年）
・電子政府ユニット（eGU: e-Government Unit）のサイト
http://www.cabinetoffice.gov.uk/e-government/
・epolitix.com（政府・地方自治体関連ニュースを取扱う）のサイト
http://www.epolitix.com/EN/
・副首相府（ODPM: Office of the Deputy Prime Minister）のサイト
http://www.odpm.gov.uk/
・IDABC（Interoperable Delivery of European eGovernment Service to public Administrations, Businesses and Citizens）のサイト
http://europa.eu.int/idabc/en/chapter/417
・地方自治 11 No.696　海外の電子自治体（2）石川義憲著（2005 年）
・t―スキームのウェブサイト
http://www.tscheme.org/about/index.html
・情報コミッショナー（IC: Information Commissioner）のサイト
http://www.informationcommissioner.gov.uk/
・改善開発庁（I&DeA: Improvement and Development Agency）のサイト
http://www.idea-knowledge.gov.uk/idk/core/page.do?pageId=1
・サウサンプトン・シティ・カウンシル（Southampton City Council）のサイト
http://www.southampton.gov.uk/