

## 参考資料

### プライバシー保護に関する先進諸外国の対応状況

本資料は、財団法人地方自治情報センターの委託事業である『電子政府・電子自治体のプライバシーに関する調査研究報告書』（平成 15 年 3 月、ネオテニー編）をもとにとりまとめたものである。

## 第 1 節 カナダにおけるプライバシー保護

### 1 カナダにおけるプライバシー保護の背景と現状

カナダにおけるプライバシー環境は、プライバシーに関する立法の状況、連邦・州による国内の法律や政策を監督する体制整備、プライバシーに関する活動家コミュニティの存在やプライバシー強化技術が発達していることなどから、プライバシー保護先進国といわれている。しかし一方で、国民はプライバシー保護に関して十分な知識を持っていない。

カナダでは、1964 年に導入された全国的な社会保険番号（SIN: Social Insurance Number）制度を有し、社会福祉の管理を行っている。

SIN の利用目的は法で制限されているが、想定外の民間商取引にも利用されているのが現状であり、何らかの対応が求められている。さらに、有効な SIN の 13%以上が何らかの形で重複しているといわれるため、不正取得の起きている可能性も高い。SIN を使った身元詐称や詐欺も発生しているが、問題の包括的調査はまだ行われていないようである。

#### 【カナダにおけるプライバシー環境の特徴】

プライバシーに関する立法（プライバシー法、個人情報保護及び電子文書法 等）  
連邦・州による国内の法律や政策を監督する体制整備（プライバシー・コミッショナー）  
プライバシーに関する活動家コミュニティの存在  
プライバシー強化技術が発達  
国民に対してプライバシー保護に関する十分な啓発を行う必要がある  
全国的な社会保険番号（SIN）制度

### 2 プライバシーに対する考え方

カナダ政府は、1982 年に制定した憲法の中で、プライバシーの権利について特別に明記はしていないが、様々な条項において示唆している。

また、プライバシーに関しては、連邦政府と州政府の双方が規制を行い、プライバシーに関する包括的な法律をはじめ、様々な法律において規制条項が盛り込まれている。

国民はプライバシー保護に十分な知識を持っているわけではなく、比較的関心は低いと言われており、公共部門に依存しているという状況である。一部では、一般市民への教育など、国民の意識を変革することに取り組むべきという意見もある。

### 3 プライバシー保護に関する対策

#### (1) 立法の状況

連邦政府が定める主要なプライバシー保護に関する法律は下表のとおりである。

##### 【連邦法の現状】

名称	時期	内容
プライバシー法	1983	連邦政府及び関連機関による個人情報の収集、使用、開示の規制、プライバシー諸原則の基本的な尊重、連邦政府機関が保有する個人情報へのアクセス権及び修正権を規定。
情報アクセス法	1985	公的に保有されている情報へのアクセスに関して定めており、情報コミッショナーによって監督されている。
プライバシー保護に関するモデルコード	1996	EU プライバシー指令 を踏まえた法律を制定しているのはケベック州のみであったため、カナダ規格協会が同モデルコードを作成し、「個人情報保護及び電子文書法 (PIPEDA*)」の条項に受け継がれた。  【モデルコードに記された 10 の指針】 責任 目的の明示 同意 収集の制限 使用、開示、保持の制限 正確性 保護 開示 個人のアクセス 遵守に関する意義申し立て
個人情報保護及び電子文書法 (PIPEDA*)	2001	連邦の規制下にある民間部門による個人情報の収集、使用、開示、あるいは州間で売買される個人情報に関して規定することを目的とする。 2001 年から段階的に適用範囲が拡大され、2004 年には商業活動で収集、使用、売買される全ての個人情報が規制対象となった。 なお、同法と基本的に同様の州立法が制定されていない場合には、この連邦法で規制される。

\* PIPEDA: Personal Information Protection and Electronic Documents Act

EU プライバシー指令では、EU 加盟国が EU 域外の諸国に個人情報を移動させるにあたって、対象国に個人のプライバシーを保護する適切な法律が存在しない限り、その移動を禁止している。

なお、州法については、国内で最もプライバシー保護が機能しているのはケベック州である。EU プライバシー指令を踏まえてカナダ国内で適切な法律を州単位で制定していたのは同州のみであり、PIPEDA と基本的に同様の法律を制定している。

## (2) 法的なスキーム

カナダでは、プライバシー法に基づき、「プライバシー・コミッショナー」を設置し、連邦議会より、カナダ国民のプライバシー権を監督・擁護する権限を与えられている。

プライバシー・コミッショナーは、プライバシー法および PIPEDA の監視に責任を負う。プライバシーに関する問題について社会を代表して仲裁を行う義務を有する。但し、プライバシーに関する問題について立法、遵守命令あるいは拘束力を持つ裁定を下す権限はない。

各州も同様の制度を設けており、その権限・義務・責任はそれぞれ異なるが基本的には同様である。

これらプライバシー・コミッショナーの活動予算は連邦あるいは州政府から用意されており、予算運用については連邦あるいは州政府の会計検査官の監査を受けることになる。

### 【プライバシーと他の重要な目標との調和】

連邦プライバシー・コミッショナーは、プライバシーの侵害や制約につながる法律を制定する際、次の4つの項目を検討するよう提案している。

項目	内容
必要性	ある特定必要性を明らかに満たすものであること
有効性	意図する目的を達成するにあたって明らかに効果的であること
応分の利益	プライバシーの侵害に見合うだけの利益をもたらすものであること
よりプライバシー侵害の少ない代替手段の欠如	同一の目標を達成するためのプライバシー侵害を抑制できる他の方法が存在しないことが明らかであること

### 【課題】

カナダは、プライバシーに関する詳細な立法措置がなされているが、法律の執行面に課題があると言われている。また、カナダのプライバシー立法の大半は比較的新しいため、まだ十分に理解されておらず、法の要求事項が完全には遵守されていないこともある。

また、州のプライバシー立法は、連邦の PIPEDA と類似の内容を持つが、詳細部分では異なっているため、州をまたがった活動をする企業にとっては障害となる場合もある。今後、連邦と州で単純かつ統一的な立法が求められている。

## (3) プライバシーと技術の現状

技術は、使い方によってプライバシーの保護にも侵害にもなり得る。カナダの連邦や州政府では、下記の技術が採用されている。

技術	内容
バイオメトリクス (Biometrics)	2002 年 6 月以降、カナダへの新規移住者には、バイオメトリクス情報 (生体認証情報) をはじめとするセキュリティ機能が組み込まれた永住者カードが交付されるようになった。 同カードには、名義人の写真と署名がレーザーで刻み込まれ、身長、

技術	内容
	目の色、性別などの身体的特徴も記入されており、世界でも最高水準の偽造困難性を有している。
データベース技術	カナダ連邦警察は、DNA サンプルデータベースを持ち、蓄積されたデータベースと犯罪現場から採取したデータを照合することで犯罪解決に役立っている。 カナダの各州及び準州は、精度の高い医療データベースを持ち、医師が全ての患者に対して適切な診断と治療を行えるよう、分かりやすく、かつ信頼できる医療情報を提供している。

【技術採用の原則：プライバシーに関わる技術を採用する際に、考慮すべき原則】

目的の把握  
 解決策には、目的の達成に必要なものだけを盛り込む  
 システムや技術が内包するプライバシーへの影響を考慮する  
 可能な限りプライバシーを保護する技術を採用する  
 技術に含まれるプライバシー強化的な性質を補完する政策をとる  
 プロジェクトの進捗に合わせてプライバシーを考える

【技術の動向】

カナダでは、プライバシー強化技術に関わる先進的な研究開発が、トロント大学やウォータールー大学、また民間の暗号技術系ベンチャー企業により行われているが、市場としてはまだ成立しているとは言い難いようである。

ただし、オンタリオ州やアルバータ州では、民間企業とともに積極的にプライバシー強化技術を開発・応用する姿勢がある。昨年より、アルバータ州政府は IBM 社と共に州政府のシステムにプライバシー強化技術を導入する開発を行っている。

【プライバシー影響評価】(PIA: Privacy Impact Assessment)

プライバシー法では、政府機関に対して予算措置の前に、新しく導入しようとする全ての技術等について、プライバシー影響評価を行うことを要求している。

評価基準

項目	内容
個人の特定性 Identity	当該の情報を用いてどの程度個人を特定できるか
データの結合性 Linkability	どれほどのデータがほかのデータと結合しているか。多くのデータが結合していれば、情報を組み合わせることで個人のプロフィールを作成できてしまう。
システムにおける観察容易性 Observability	システムを本来の用途で使用した際、どれほど容易に個人を識別できるか。また、他のデータへの繋がりをどれだけ発見できるか。

プライバシー影響評価の要件（例）

項目	内容
公正情報処理規定	経済協力開発機構(OECD)では 8 項目、カナダをはじめとする地域では 10 項目とされている公正情報処理規定。
法令で定められたプライバシー要件	法令で定められたプライバシー要件を記載。 広く一般を対象としたプライバシー法(例：カナダの「 <u>個人情報保護と電子文書法</u> 」( <u>Personal Information Protection and Electronic Documents : PIPED Act</u> ))、特定のセクターや産業に限定して適用される法令(例：カナダの「 <u>オンタリオ州健康保険法</u> 」( <u>Ontario Health Insurance Act</u> )、「 <u>銀行法</u> 」( <u>Bank Act</u> )」など)
契約に関するプライバシー要件	プロジェクトで役割を担う個人や組織が従う必要のある契約上の義務を記載。
その他のプライバシー要件	その他のプライバシー要件を記載。例えば、業界慣行、産業団体の勧告、行動規範、各種ポリシー、規制当局(医師及び看護師の規制を担当する「ヘルスカレッジ」(health college)等)など。
プロジェクトの設立要綱、公約及び前提条件	プロジェクトの設立要綱で定められた前提条件、プライバシー保護のためになされた公約を記載。
既決のポリシー	既に決定されているポリシーを記載。

## 第2節 アメリカ合衆国におけるプライバシー保護

### 1 アメリカ合衆国におけるプライバシー保護の背景と現状

連邦・州・地方自治体がそれぞれに定めたプライバシーに関する法律や規則が多く存在しており、統一は難しいようである。産業界では、クレジットや金融サービス等の分野における最小限の法律を守る以外は、ビジネス上で生じるプライバシー侵害に関し自主的規制による。しかし、集団訴訟と社会的評価に基づく株価変動が企業活動に大きな圧力を与えている。

米国では、社会保障番号（SSN: Social Security Number）が重要な影響を持っている。SSNは元来、政府による年金と徴税のため個人の経済活動を記録し追跡する手段であるが、現在は想定外の民間などあらゆる場面で万能の個人識別番号として使われているため、悪意ある者の手に渡るとその被害は大きくなり、実際にも成り済まし犯罪が増加している状況がある。

また、最も広く使われている身分証明証として使われている運転免許証、州が発行するIDカードがあるが、今後のバイオメトリクス情報の追加については賛否の意見が出ている。

### 2 プライバシーに対する考え方

最近の「対テロ」を追い風に、市民的自由とプライバシーを制限する法律の成立が法執行機関から期待されるようになっており、「USA パトリオット法」や「国土安全保障法」が施行されたが、テロとは関係のない捜査の目的で適用されないことが求められている。

### 3 プライバシー保護に関する対策

#### （1）立法の状況

法律	時期	内容
プライバシー法	1974	市民の個人情報の使用や開示にあたり、連邦政府諸機関が一定のガイドラインに従い、政府による市民のプライバシー尊重を目的とする。個人情報のデータファイルの管理にあたり、データベースやシステムの利用について説明責任及び監視を推進する。
プライバシー保護法	1980	メディア組織の事務所や職員の記録、その他の情報へのアクセスを求める際に、法律の執行について法的手続きを求めている。一般的に、州、連邦双方の職員が、ジャーナリストが所有する著作物や文書資料を捜索、差し押さえることを禁止しており、法的措置のためには、裁判所の召喚状を得なければならないとしている。
その他の法律	-	公正信用報告法（1970）、家族の教育上の権利およびプライバシー法（1974）、情報公開法（1974）、外国諜報活動偵察法（1978）、金融プライバシー権法（1978）、ケーブル通信政策法（1984）、電子通信プライバシー法（1984）、ビデオ・プライバシー保護法（1988）、嘘発見器使用からの従業員保護法（1988）、電話加入者保護法（1991）、運転免許プライバシー保護法（1994）、電気通信法（1996）、子供のオンライン上のプライバシー保護法（1998）、金融サービス近代化法（1999）、連邦取引委員会法（1914）、健康保険に関する携行性および説明責任に関する法（1996、2002）、電子政府法（2002）

#### （2）法的なスキーム

米国には、国内居住者のプライバシー問題をあらゆる角度から把握している機関はないが、企業と消費者に関する問題については連邦取引委員会が積極的な調査と対応を行う。

### 第3節 ヨーロッパにおけるプライバシー保護

#### 1 ヨーロッパにおけるプライバシー保護の背景

##### (1) 欧州人権条約

1950年の欧州人権条約において、批准国内におけるプライバシー権が定められている。プライバシー権の保護は、欧州人権条約により最優先で保護される憲法上の権利である。同条約は、プライバシー保護強化に向けた下記の二つの動きを支えてきた。

欧州人権裁判所は、各国の法律を検証し、プライバシー保護が適切に行われていない国々に対して、制裁を課してきた。

欧州では、データ保護法という形式のプライバシー規定が多数制定されている。(これらの法律が1995のEUデータ保護指令に繋がった)

##### 【欧州人権条約第8条】

(1)すべての者は、その私生活、家族生活、住居および通信の尊重を受ける権利を有する。  
(2)この権利の行使に対しては、法律に基づき、かつ国の安全、公共の安全もしくは国の経済的福利のため、混乱もしくは犯罪の防止のため、健康もしくは道徳の保護のため、または他者の権利および自由の保護のため民主的社会において必要な場合以外、公的機関による干渉があってはならない。

##### (2) EU 個人データ保護指令 (Directive95/46/EC)

EU 個人データ保護指令は、EU 各国におけるプライバシー規定を受けて、一貫した保護水準を市民に提供し、EU 単一市場内におけるデータの自由な流通を保障している。

また、EU 域外の諸国に個人情報を移動させるにあたって、対象国に個人のプライバシーを保護する適切な法律が存在しない限り、その移動を禁止している。

EU 加盟国は、プライバシー、データ保護、人権に関する取り決めに支持する義務を有しており、各国は一連の共通基準を満たす国内法を成立させる必要がある。

##### 【EU 指令で定められた公正情報処理規定】

- ・データは公正かつ適法に処理されなければならない。
- ・データは明示的かつ合法的な目的において収集され、その目的に沿って使用されなければならない。
- ・データは処理される目的に鑑みて適切なものでなければならず、過度であってはならない。
- ・データは正確でなければならず、必要に応じて更新されなければならない。
- ・データ管理者は、データ主体に対し、自身についての不正確なデータを修正、消去、またはブロックするための適切な手段を提供しなければならない。
- ・個人を特定するデータは、必要期間以上保持されてはならない。
- ・同指令では、加盟国は指令の適用を監視するための監督機関を複数設置しなければならないと定められている。監督機関には公的な登録情報を更新し、すべてのデータ管理者の氏名およびデータ処理方法に一般市民がアクセスできるようにする義務がある。

- ・原則的には、すべてのデータ管理者はデータ処理を行う際に監督機関に報告しなければならない。特定の危険を伴わない種類の処理については加盟国の判断により、報告の簡略化および免除を適用することが可能である。報告の免除および簡略化は、国内法令に基づき管理者によりデータ保護の責を負う独立した役員が指名された場合においても認められる。

## 2 ユーロッパにおけるプライバシーに対する考え方

欧州の各種データ保護法は全般に、適切なデータ保護の重要性を認識している点で最も進んでいるとされているが、プライバシーに関する権利は、表現や移動の自由等の権利に比べて公益性の認識は高くないと言われている。

## 3 ユーロッパにおけるプライバシーと技術

欧州において、プライバシー強化技術は、何より EU データ保護指令に照らして理解されるべきものと位置付けられている。しかし、欧州におけるプライバシー技術の実際の採用見通しおよび有効性は現時点では不透明である。経済協力開発機構（OECD）が行ったプライバシー強化技術に関する調査では、大半の加盟国ではプライバシー保護技術は限定的に導入されているというものであった。

一方で、欧州委員会と EU 加盟国、欧州議会は、Framework Programmes for Research and Technological Development（FP：研究フレームワークプログラム）により、技術研究、開発を推進している。2002 年から 2006 年を年限として、その第 6 次 FP（FP6）が進められている。

この中で、下表に示すようなプライバシー保護技術に関するプロジェクトが進められている。

### 【ヨーロッパにおけるプライバシー保護技術に関する代表的なプロジェクト】

取り組み	内容
P3P: Platform for Privacy Preferences	オンラインユーザーに、プライバシー参照権の管理を可能とする技術である。ユーザーがどこまでの情報を開示範囲とするかを設定すると、ブラウザに設定された P3P が、サーバー内のプライバシーポリシーとやりとりし、サーバー上の開示範囲を設定する。このことにより、本人がより直接的に開示範囲を管理することが可能になる。
GUIDES : best practice guidelines for adherence to the EU directives	欧州の e ビジネス企業が EU のデータ保護の仕組みに沿った行動をとるための手引きとなる、実用的なガイドラインである。 おもに、http プロトコル（Web ブラウザ、OS、IPv6 を含む）や Web のバグ、クッキー、電子プロファイリングについての技術的な指針を示している。
PRIDEH : Privacy Enhancement in Data Management in E-Health	健康管理業界をターゲットとしたプライバシー強化技術である。 情報管理の「鍵」として身元情報が活用されていることがプライバシー問題につながっているという点に、問題意識を持って研究・開発が進められている。具体的には、Trusted Third Party（TTP：信頼できる第三者機関）が匿名の「鍵」を提供することにより、プライバシー侵害を最小限化することを目指している。 本技術は、将来的には、他の業界も視野に入れている。



取り組み	内容
PISA : Privacy Incorporated Software Agent	ユーザーのプライバシーを保護するための電子的仲介機能を開発することを目的としたプロジェクト。プライバシーの保護には、法的保護や自己規制のみでなく、プライバシー強化技術が必要であるとし、以下のような技術を実証モデルとして組み込んでいる。 ・インテリジェントな検索及びマッチングのためのエージェント技術 ・プロファイルを作成し予測するためのデータ ・マイニングまたは同等の技術 ・取引の守秘性および個人データの保護のための暗号化技術
PAMPAS : Pioneering Advanced Mobile Privacy and Security	2003 年の PF6 でさらなる研究を進めるために、モバイル環境におけるプライバシーとセキュリティのフレームワークの構築を目的としたプロジェクト。プライバシーや ID の管理についての研究の必要性を主張している。
RAPID : Roadmap for Advanced research in Privacy and IDentity Management	業界、教育機関、研究所、人権擁護団体等の専門家から構成されるプロジェクト。 プライバシーが保護された世界を実現するための技術的、法的、方法的基盤を構築することを目的としている。有用性やセキュリティといった他の条件も尊重しつつ、市民のプライバシーを真に保護する活力あるシステムを作り上げることを、長期的な目標としている。

また、ドイツでは、経済技術省がオンライン技術の匿名利用を奨励するプログラムを実施している。また、オランダでは政府が新しい公共データ処理システムにプライバシー強化技術を採用する意向を明らかにしている。

#### 【ドイツのプライバシー強化技術開発一覧】

技術	内容
GnuPG	Gnu Privacy Guard 暗号化プロジェクトへのドイツ人の参加
GnuPP	Gnu Privacy Project の略。2002 年にスタートした一般向け GnuPG。
Steganography	ステガノグラフィー・アルゴリズムおよびツールの開発
BioTrusT	プライバシー準拠バイオメトリクスの研究および開発。
Anonymous Biometrics	ユーザーのチップガード上のバイオメトリック・データを保護するための暗号メカニズム
AN.ON	Anonymity online-Strong Anonymity and Unobservability in the Internet の略。オープンソース・ユーザ・ソフトウェアとミックス・インフラストラクチャーの開発と運営。
Rewebber	匿名プロキシ。（ハーゲン放送大学が開発したもの）
DRIM	Dresden Identity Management の略。PRISMA の一部。
PRIMA	ID 管理プロキシの試作品。
PRISMA	Privacy-Rich Identity and Security Management の略。変換可能なクレデンシャルを統合するプライバシー強化 ID 管理リファレンス・アーキテクチャの設計。法的、社会学的、ユーザビリティの各側面に関する研究を行う。
DASIT	Datenschutz in Telediensten(Data Protection in Tele Services)の略。ユーザーによるオンライン・プライバシー権主張を支援する試作品を開発。

## 4 デンマークにおけるプライバシー保護に関する対策

### (1) デンマークにおけるプライバシー保護の背景と現状

デンマークにおける社会背景として、国民の政府に対する信頼が高水準であること、給付金詐欺やテロ対策に力を入れつつあることが挙げられる。デンマークでは、国民は法によりプライバシー保護を受けている。

またデンマークでは、1968 年から国民 ID 番号（CPR:Central Person Register 番号＊）制度を採用しており、現在、国民生活の様々な場面で識別子として使用されている。

しかし、効率性を向上させるため電子政府化の加速に努力が払われてきているため、行政の部門横断的データ処理に向かいつつあり、信頼と法的保護だけでは支え続けられないのではないかという懸念が出てきているようである。

＊CPR 番号：「中央個人登録番号」。個人の生年月日に 4 桁を足した数字で構成。行政分野や商業活動でも利用され、税務当局への申告や雇用、医療、行政サービスなどで利用される。

### (2) プライバシー保護に関する対策

デンマークでは、1953 年改正の憲法の中にプライバシーの権利を明文化している。欧州の全ての国が憲法の中にプライバシーの権利を明文化しているわけではない。

下表のような法律が整備されているほかにも、プライバシーを保護する法律はいくつかあり、個人情報の取り扱いに関する基本原則についても規定している。

法整備の状況

項目	時期	内容
デンマーク憲法	1953（改正）	プライバシーの権利を明文化
民間登録法	1978	データ保護における公共部門の役割が規定された
個人データ処理に関する法律	2000	EU 個人データ保護指令を履行する国内法

なお、国民のプライバシーは、複雑な法的システムに支えられており、プライバシー強化技術導入の試みは殆ど見られない。2002 年にデンマーク消費者委員会は、消費者のプライバシーをデジタル化による脅威から守るために技術的解決を政策に求めたが、まだ導入はされていない。

体制：「データ保護庁」

公共および民間のデータベースや各種登録を監督する機関であり、またプライバシーに係る新法令が発布される場合に見解を示す。

## 5 フィンランドにおけるプライバシー保護に関する対策

### (1) フィンランドにおけるプライバシー保護の背景と現状

フィンランドでは、国および地方自治体の情報開示についてオープンな政策をとっており、情報へのアクセス権は法律に明記されており、政府における情報開示及び適切な情報管理の推進、個人や組織に対する監視の機会等が義務付けられている。

一方、フィンランドでは、「国民識別番号制度」を擁しており、パスポート、運転免許証など様々なデータファイルで官民間問わず広く利用されている。また、1999年に政府の保証するデジタル証明書データを含む有効期限3年のICカードを発行しているが普及率は低いといわれる。これらの情報が全て政府のデータベースとなる動きに対して、プライバシー保護の観点から懸念が生じている。

フィンランドには数々のセキュリティやバイオメトリクス、スマートカードの企業があるが、プライバシー強化技術としては積極的な導入はまだ行われていないようである。

### (2) プライバシー保護に関する対策

デンマークと同様に、憲法にプライバシーの権利が明文化されている。全ての個人について、その私的な生活、尊厳、住居を保護している（フィンランド憲法政体法第8条）。

#### 法整備の状況

項目	時期	内容
個人データ保護法	1999 改正	1987年に可決した「個人データファイル法」について、EU指令に準拠させる目的で改正されたもの。改正により、情報の使用と開示にあたり本人による事前の同意及び情報についての自己決定を規定している。
電子署名法	2003	特定の方法で作成された電子署名は、手書きの署名と同じ効力を持つ。

体制：「データ保護オンブズマン」

執行力のあるプライバシー問題専門家として政府が設置した。データ保護オンブズマン及びその事務局は、個人データ処理に関するあらゆる問題について、指導・助言を行うとともに、法律の遵守状況を監視している。

## 6 フランスにおけるプライバシー保護に関する対策

### (1) フランスにおけるプライバシー保護の背景と現状

フランスでは、プライバシー権は、1958年憲法では明文化されていない。しかし、フランスで最初にプライバシー権が認知されたのは19世紀であり、1994年に憲法院において、この権利は暗黙のうちに認められているという判断が下されている。1974年にデータ保護法が成立し、1978年にデータプライバシー・コミッション(CNIL)が設置された。CNILは、「相互利用禁止」の立場をとり、データベース間の結合を作る試みに対してほぼ反対し、成果を上げてきたようである。

プライバシーに対する考え方におけるフランスの特徴としては、「暗号は政府が所有すべ

きものと見なされていること」、「国内においてスマートカードには長い歴史があること＊」が挙げられる。

また、フランスはこれまで「行政の電子化」に関して多くのイニシアティブをとっており、「情報社会に向けた国家計画（1998）」「RE / SO 2007 計画（2002）」を策定するとともに数多くの政令・省令・通達を作るなど、電子政府の推進に努めている。

PKI（公開鍵基盤）については、金融、信用機関によるコンソーシアムや民間 PKI 企業が積極的に活動している。フランス経済・財政・産業省が導入した付加価値税納税システム (TeleTVA) が拡大の刺激になっているといわれる。

＊スマートカード：フランスでは PIN コードが必要なチップが埋め込まれたクレジットカードが 20 年以上も使われている。スマートカードには電子財布「Moneo」が含まれており、利用者は電子マネーにより小額の買い物も可能である。銀行の依頼があれば、「Moneo」は利用者の取引データ、販売時点情報などの詳細を全て記録できる。

## （２）プライバシー保護に関する対策

### 法整備の状況

項目	時期	内容
データ保護法	1974	プライバシーを公的・私的な侵害から保護する法律。EU 指令を遵守する国内法として修正の論議がなされている。

体制：CNIL

プライバシーを公的・私的な侵害から保護する法律として、データ保護法が制定されるとともに、体制として、1978 に「情報処理と自由のための国民委員会(CNIL)」が設置された。

## 7 イギリスにおけるプライバシー保護に関する対策

### （１）イギリスにおけるプライバシー保護の背景と現状

イギリスは成文憲法を持たないという点で他の諸国と異なる。同国では、プライバシー強化技術の利用は限定的なようである。

「エンタイトルメント・カード」と呼ばれる事実上の国民 ID カードの導入に際しては、国民の関心が向けられたが、その導入の影響に対処し得る技術への関心に向かうまでは至っていない。1997 年に国民保健サービスのカルディコット委員会が、医療情報分野でのプライバシー強化技術の利用を促す提言をしたが、ほとんど実行に移されていないようである。

## ( 2 ) プライバシー保護に関する対策

### 法整備の状況

項目	時期	内容
データ保護法	1984 1998 改正	EU 指令の要件を満たす。公共部門と民間部門の双方の活動に関して規定しており、情報コミッショナーが法の執行にあたる。
人権法	1998	欧州人権条約に沿った国内法。英国の法律において、初めてプライバシー権に関する規定が設けられた。
調査権限規定法	2000	プライバシー侵害にあたる規則と見る向きもある。内務省の長に通信の傍受に必要な令状を発行する権限を与えている。

体制：「情報コミッショナー事務局」

プライバシー保護に関しては、情報コミッショナー事務局が責任を負うこととされている。データの使用者の登録簿を管理し、法の執行にあたる。

### 【技術の動向】

イギリスでは、プライバシー強化技術や暗号についての研究はケンブリッジ大学やオックスフォード大学で比較的盛んでありレベルは高いが、製品を手掛ける企業数は限られており、この技術を取り巻く市場は伸びていない。IPv6 や PKI 等の技術の採用に関する検討状況は下記のとおりである。

技術	採用に関する検討状況
IPv6 ( インターネットプロトコル・バージョン 6 )	イギリスにおいて広く普及するまでに至っていないが、複数の研究機関のネットワークにおいて数年前から試験運用されている。
PKI ( 公開鍵基盤 )	政府が同技術を用いて「キー・エスクロー ( 暗号鍵の寄託 )」の義務付けを検討したが、セキュリティ上のリスクから反対を受け、計画が見送られた。
暗号化	調査権限規定法により、イギリスの法執行機関は複合鍵の提示や暗号データの複合化を要求する権限を有している。こうした権限に対してアクセスし得る情報の量を最小限に抑えるための技術開発が進められている。

注) 英文での「Privacy」の訳語は、すべて「プライバシー」とした。