

電子商取引における個人情報の 保護に関する中間報告

- 民間部門における電子商取引に係る個人情報の
保護に関するガイドライン(アルファ版) -

平成 9 年 5 月



電子商取引実証推進協議会
プライバシー問題検討WG

目 次

1 プライバシー問題ワーキンググループについて	1
1.1 概要	1
1.2 目的	1
1.3 検討範囲	1
2 はじめに	2
3 民間部門における電子商取引に係る個人情報の保護に関するガイドライン（アルファ版）	3
4 海外調査報告	9
4.1 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT(OECD)	10
4.1.1 組織の概要	10
4.1.2 トピックス	10
4.1.3 調査内容	12
4.2 EUROPEAN UNION(EU)	15
4.2.1 組織の概要；	15
4.2.2 調査内容	16
4.3 ドイツ銀行協会 BUNDESNERBAND DEUTSCHER BANKEN(BDB)	18
4.3.1 組織の概要；	18
4.3.2 調査内容	18
4.4 THE DATA PROTECTION REGISTRAR	22
4.4.1 訪問先概要；	22
4.4.2 調査内容	23
4.4.3 電子商取引との関連	27
4.5 英国内務省 HOME OFFICE（DATA PROTECTION SECTION）	27
4.5.1 組織の概要；	27
4.5.2 調査内容	28
4.6 カナダ産業省 INDUSTRY CANADA	30
4.6.1 組織の概要	30

4.6.2	トピック.....	31
4.6.3	調査内容.....	31
4.7	アメリカ EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET	33
4.7.1	組織の概要.....	34
4.7.2	調査内容.....	34
4.8	アメリカ COMMERCE NET (ETRUST)	36
4.8.1	組織の概要 ;	36
4.8.2	トピック.....	37
4.8.3	調査内容.....	37
4.8.4	電子商取引との関連.....	39
5	参考資料	39
5.1	OECDガイドラインの和訳	39
5.1.1	プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告 (1980年9月).....	40
5.1.2	プライバシー保護と個人データの国際流通についてのガイドライン	40
5.2	個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理 事会の指令(EU指令).....	44
5.2.1	EU指令の和訳.....	45
6	ワーキンググループメンバー名簿.....	70

1 プライバシー問題ワーキンググループについて

1.1 概要

電子商取引においては、これまで以上に個人情報がオープンなネットワークを通じて、収集され、利用されることが予想される。電子商取引は、事業者並びに消費者に利益をもたらすことが期待される反面、個人情報等の漏えい等について懸念されている。

そこで、当ワーキンググループでは、個人情報の保護に関連した国内外の制度等について調査・分析し、電子商取引に係る個人情報の保護の為のガイドラインを作成することとした。

1.2 目的

- (1) 個人情報保護の施策を制度面・技術面・国際面より検討し、健全な電子商取引の普及を図る。
- (2) 個人情報保護のガイドラインを策定し、安心かつ信頼できる電子商取引の普及を促進する。

1.3 検討範囲

通商産業省が策定した「民間部門における電子計算機処理に係る個人情報の保護についての指針改正案について（意見照会）」をもとにし、「民間部門における電子商取引に係る個人情報の保護に関するガイドライン（アルファ版）」を作成した。今後、実証実験プロジェクト並びに一般の方々の意見を求め、より実効性を高めた電子商取引における個人情報の保護のガイドライン（最終版）を策定する。

さらに、今後の活動として、事業者並びに消費者から見てわかりやすい、ガイドラインの解説書及びモデルホームページを例示することを考えている。

また、電子商取引の魅力の一つとして国際間取引があり、これに伴い国際間で個人情報の移転が行われる。従って、外国関係機関との連携も必要と考えられ、適宜に情報を交換しながら、個人情報が侵害されたときの救済制度について検討を進める。

2 はじめに

パソコンが急速に普及し、インターネットを使った電子商取引の拡大が期待されている。一方で従来のオフラインにおけるコンピュータ処理にたいして、オープンネットワークの中でコンピュータ処理される商取引に伴う購入履歴情報を含めた個人情報、ネットワークを通じて容易に収集されるのではないかという不安視されている。われわれの個人情報について、適切な保護がされる保障がない限り、消費者は電子商取引の世界へ足を運びいれることを躊躇うであろう。

また、電子商取引は、グローバルな運営が特徴の一つでもあり、国内の事情だけでなく国際的な観点からも個人情報の保護を考えなければならない。

世界に目を向けると、1980年の経済協力開発機構(OECD、1997年2月現在29ヶ国加盟)のプライバシー・ガイドライン勧告以降、各加盟国は個人情報保護法を制定してきている。また、ヨーロッパにおいては、1995年10月に「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」(以下、EU指令という)が採択された。この指令の中には、第三国へのデータ移転について厳しい要件を課したものがあり、欧州連合だけに限らず我が国においても大きな影響があると考えられる。なお、この指令の採択を契機に、これまで民間部門においては民間の自主規制に任せていたカナダやオーストラリアの国々も法律化に踏み切っている。

このように個人情報・プライバシーの保護に関しては、世界の各国の潮流は法律化にある。いまだ民間部門の個人情報の保護についての法律が無く、すぐには法律の制定の見込の無い日本では、従来よりガイドラインによる自主規制で対応してきている。

このような状況下において、1996年12月に通商産業省で公表し、一般の人々から意見を求めた『民間部門におけるコンピュータ処理に係るプライバシー保護について』は、従来のガイドラインをより詳細に、且つEU指令への適応を図る改正であった。このガイドラインの対象は、通商産業省が所管する業界で使用され、実効をあげるものである。

一方、電子商取引は、事業者にとって出店コストの負担が軽く、また低コストで広範囲に宣伝効果を得られるという魅力から、これまで通信販売を行っている事業者に加え、業界に属さない個人や小規模の企業の出店が予想される。これら出店者が必ずしも個人情報の保護の取扱いについて、精通しているわけではないだろう。

そこで、商取引に伴って初めて個人情報の保護を取扱う事業者に対する指針として、通商産業省の作成したガイドラインを基にし、それを補完、かつ一部対象を重複しながら、

個人情報の保護の実効性をあげる為のガイドラインを作成することとした。このガイドラインは、個人情報の取扱を、収集・利用・提供・管理の局面から、それぞれについて規定している。

このガイドラインの特徴としては、

オンラインのネットワークによる情報のやり取りを重点的な対象としていること。

電子商取引で個人情報を取扱う全てのものを対象とし、従来の企業を意識したものから、個人事業者まで対象範囲を広げていること。

電子商取引では、アクセスしただけでも個人情報を特定することが出来ることから、商取引の範囲を売買だけではなく、これを誘引する広告・宣伝も含めると定義したこと。

等があげられる。

電子商取引がより一層普及する為には、個人情報保護は欠かせない問題と認識されている。そういう意味において、この「電子商取引における個人情報の保護に関するガイドライン(アルファ版)」は、電子商取引に的を絞った個人情報保護施策として、世界に先駆けた取組みと自負している。

今後の活動としては、通商産業省が支援する電子商取引実証実験プロジェクト及び一般に広く意見を求め、より実効性を高めたガイドライン(最終版)を策定する。

なお、今回のガイドライン策定にあたっては、諸外国等における個人情報の保護の現状ならびに電子商取引における検討状況等の調査を行った。この調査報告を読まれ、個人情報保護について検討される際の、参考にされることを願うものである。

3 民間部門における電子商取引に係る個人情報の保護に関するガ

イドライン（アルファ版）

第1章 ガイドラインの目的

（目的）

第1条 このガイドラインは、電子商取引において取り扱う個人情報の適切な保護を図ることを目的とする。

第2章 定義

（定義）

第2条 このガイドラインにおいて、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- （1）電子商取引 電子的ネットワーク上で行われる商取引及びこれを誘引するための宣伝・広告の一部又は全部を行うことをいう。
- （2）個人情報 個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号、画像若しくは音声により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む）をいう。
- （3）管理者 電子商取引において、個人情報の収集、利用又は提供の目的及び手段等を決定する権限を有する者をいう。
- （4）受領者 個人情報の提供を受ける者をいう。
- （5）情報主体の同意 情報主体が、自己に関する個人情報の取扱いを承諾する意思表示を行うことをいう。

第3章 ガイドラインの適用範囲

（対象となる個人情報）

第3条 このガイドラインは、電子商取引において、その全部又は一部が電子計算機、光学式情報処理装置等の自動処理システムにより処理されている個人情報を対象とし、自動処理システムによる処理を行うことを目的として書面等により処理されている個人情報についてもこれを適用する。

（ガイドラインの拡張）

第4条 このガイドラインは、個人情報の適切な保護の目的の範囲内において業種、事業等の活動の実態に応じた項目を追加し、又は修正することができる。

第4章 個人情報の収集に関する措置

(収集範囲の制限)

第5条 個人情報の収集は、電子商取引において個人情報の利用者がその正当な業務の範囲内で、収集目的を明確に定め、その目的の達成に必要な限度においてこれを行うものとする。

(収集方法の制限)

第6条 個人情報の収集は、適法かつ公正な手段によって行うものとする。

(特定の機微な個人情報の収集の禁止)

第7条 次に掲げる種類の内容を含む個人情報については、これを収集し、利用し又は提供してはならない。ただし、当該情報の収集、利用又は提供についての情報主体の明確な同意がある場合は、この限りでない。

- (1) 人種及び民族
- (2) 門地及び本籍地(所在都道府県に関する情報を除く)
- (3) 信教(宗教、思想及び信条)、政治的見解及び労働組合への加盟
- (4) 保健医療及び性生活

(情報主体から直接収集する場合の措置)

第8条 情報主体から直接に個人情報を収集する際には、情報主体に対して、少なくとも、次に掲げる事項又はそれと同等以上の内容の事項を明示し、当該個人情報の収集、利用又は提供に関する同意を得るものとする。ただし、既に情報主体が、次に掲げる事項の通知を受けていることが明白である場合及び情報主体により不特定多数の者に公開された情報からこれを収集する場合には、この限りでない。

- (1) 個人情報に関する管理者又はその代理人の氏名又は職名、所属及び連絡先
- (2) 個人情報の収集及び利用の目的
- (3) 個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又

は受領者の組織の種類、属性及び個人情報の取扱いに関する契約の有無

(4) 個人情報の提供に関する情報主体の任意性及び当該情報を提供しなかった場合に生じる結果

(5) 個人情報の開示を求める権利及び開示の結果、当該情報が誤っている場合には訂正又は削除を要求する権利の存在及び当該権利を行使するための具体的方法

(情報主体以外からの間接的に収集する場合の措置)

第9条 情報主体以外から間接的に個人情報を収集する際には、情報主体に対して、少なくとも、前条(1)から(3)まで及び(5)に掲げる事項を明示し、当該個人情報の収集、利用又は提供に関する同意を得るものとする。ただし、次の(1)から(4)までのいずれかに掲げる要件を満たす場合においては、この限りではない。

(1) 情報主体からの個人情報の収集時に、あらかじめ自己への情報の提供を予定している旨前条(3)に従い情報主体に通知した提供者から収集を行う場合

(2) 提供される個人情報に関する守秘義務、再提供禁止及び事故時の責任分担等の契約の締結により、個人情報に関して提供者と同等の取扱いを担保することによって個人情報の提供を受け、収集を行う場合

(3) 既に情報主体が、前条(1)から(5)までに掲げる事項の通知を受けていることが明白である場合及び情報主体により不特定多数の者に公開された情報からこれを収集する場合

(4) 正当な業務の範囲内であって、情報主体の保護に値する利益が侵害されるおそれのない収集を行う場合

第5章 個人情報の利用に関する措置

(利用範囲の制限)

第10条 個人情報の利用は、第12条の場合を除き、収集目的の範囲内で行うものとする。

(目的内の利用の場合の措置)

第11条 収集目的の範囲内で行う個人情報の利用は、次の(1)から(4)までに掲げ

るいずれかの場合にのみこれを行うものとする。

- (1) 情報主体が同意を与えた場合
- (2) 情報主体が当事者である契約の準備又は履行のために必要な場合
- (3) 企業ならびに個人等が従うべき法的義務のために必要な場合
- (4) 情報主体の生命、健康及び財産等の重大な利益を保護するために必要な場合

(目的外の利用の場合の措置)

第12条 収集目的の範囲を超えて個人情報の利用を行う場合又は前条(1)から(4)までに掲げるいずれの場合にも当たらない個人情報の利用を行う場合においては、少なくとも、第8条(1)から(3)まで及び(5)に掲げる事項を明示し、あらかじめ情報主体の同意を得、又は利用より前の時点で情報主体に拒絶の機会を与える等、情報主体による事前の了解の下に行うものとする。

第6章 個人情報の提供に関する措置

(提供範囲の制限)

第13条 個人情報の提供は、原則として収集目的の範囲内で行うものとする。

(目的内の提供の場合の措置)

第14条 収集目的の範囲内で行う個人情報の提供は、少なくとも、第8条(1)から(3)まで及び(5)に掲げる情報を明示し、あらかじめ情報主体の同意を得、又は提供より前の時点で情報主体に拒絶の機会を与える等、情報主体による事前の了解の下に行うものとする。ただし、次の(1)から(4)までに掲げるいずれかの場合においては、この限りでない。

- (1) 情報主体からの個人情報の収集時に、あらかじめ当該情報の提供を予定している旨第8条(3)に従い情報主体の同意を得ている受領者に対して提供を行う場合
- (2) 提供した個人情報に関する守秘義務、再提供禁止及び事故時の責任分担等の契約の締結により、個人情報に関する自己と同等の取扱いが担保されている受領者に対して提供を行う場合
- (3) 受領者が当該個人情報について改めて第8条(1)から(5)までに掲げる事項を提供し、情報主体の同意を得る措置を採ることが明白である場合

(4) 正当な業務の範囲内であって、情報主体の保護に値する利益が侵害されるおそれのない提供を行う場合。

(目的外の提供の場合の措置)

第15条 収集目的の範囲を超えて個人情報の提供を行う場合又は前条(1)から(4)までに掲げるいずれの場合にも当たらない個人情報の提供を行う場合においては、情報主体に対して、少なくとも、個人情報の受領者に関する第8条(1)から(3)まで及び(5)に相当する事項を明示し、情報主体の同意を得るものとする。この場合において、第8条(3)中「提供」とあるのは「再提供」と読み替えるものとする。ただし、既に情報主体が、当該情報の通知を受け包括的な同意を与えていることが明白な場合は、この限りでない。

第7章 個人情報の適正管理義務

(個人情報の正確性の確保)

第16条 個人情報は、利用目的に応じ必要な範囲において、正確かつ最新の状態で管理するものとする。

(個人情報の利用の安全性の確保)

第17条 個人情報への不当なアクセス又は個人情報の紛失、破壊、改ざん、漏えい等の危険に対して、技術面及び組織面において合理的な安全対策を講ずるものとする。

(個人情報の秘密保持に関する従事者の責務)

第18条 個人情報の収集、利用及び提供に従事する者は、法令の規定又は管理者が定めた規定若しくは指示した事項に従い、個人情報の秘密の保持に十分な注意を払いつその業務を行うものとする。

(個人情報の委託処理に関する措置)

第19条 情報処理を委託する等のため個人情報を外部に預託する場合においては、十分な個人情報の保護水準を提供する者を選定し、契約等の法律行為により、管理者の指示の遵守、個人情報に関する秘密の保持、再提供の禁止及び事故時の責

任分担等を担保するとともに、当該契約書等の書面又は電磁的記録を個人情報の保持期間にわたり保存するものとする。

第8章 自己情報に関する情報主体の権利

(自己情報に関する権利)

第20条 情報主体から自己の情報について開示を求められた場合は、原則として合理的な期間内にこれに応ずる。また開示の結果、誤った情報があった場合で、訂正又は削除を求められた場合には、原則として合理的な期間内にこれに応ずるとともに、訂正又は削除を行った場合には、可能な範囲内で当該個人情報の受領者に対して通知を行うものとする。

(自己情報の利用又は提供の拒否権)

第21条 既に保有している個人情報について、情報主体から自己の情報についての利用又は第三者への提供を拒まれた場合は、これに応ずるものとする。但し、管理者若しくは個人情報の開示の対象となる第三者等の法令に基づく権限の行使又は義務の履行のために必要な場合については、この限りでない。

第9章 管理体制

(管理者の指名)

第22条 このガイドラインの内容を理解し実践する能力のある者を内部から1名以上指名し、個人情報の管理者としての業務を行わせるものとする。

(管理者の責務)

第23条 個人情報の管理者は、このガイドラインに定められた事項を理解し、及び遵守するとともに、従事者にこれを理解させ、及び遵守させるための教育訓練、内部規定の整備、安全対策の実施並びに実践遵守計画(コンプライアンス・プログラム)の策定及び周知徹底等の措置を実施する責任を負うものとする。

4 海外調査報告

調査期間；1997年2月9日～21日

調査メンバー；堀部一橋大学教授（WG12主査）、佐草（WG12副主査）、東（WG1主査）、関本（（財）日本情報処理開発協会 情報セキュリティ対策室課長）、巽（（財）金融情報システムセンター 調査企画部調査役）

4.1 Organisation for Economic Co-operation and Development(OECD)

4.1.1 組織の概要

1961年9月に発足した国際機関で、主なねらいは加盟国の協力によって経済の安定成長と貿易拡大につとめ、さらに加盟国による発展途上国援助の促進と調整を図ることにある。加盟国は、1997年2月現在で29カ国となっている。

最高機関は理事会で下部組織として各種の委員会が設置されている。

- 訪問先住所；37 bis,boulevard suchet 75016 PARIS
- 訪問日時；1997年2月10日（月）10時～12時
- 対応者；
 - (1) Information,Computer and Communications Policy (ICCP)
 - ・ John Dryden
 - ・ Hiroko Kamata
 - ・ Teresa Peters
 - ・ Akio Onisi
 - (2) Consumer Policy (CCP)
 - ・ Elizabeth Lynch

- 訪問目的

1995年10月に採択された「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（EU指令）を受けた各国の国内法の整備状況とOECDにおける個人データ保護に関する活動状況を調査する。

4.1.2 トピックス

電子商取引はOECDにとっても重要なテーマと考えている。

OECDでは、以下のプライバシー保護を行った。

- 1980年 個人情報保護のガイドラインを作成。
- 1985年 データの伝達に関するOECDの宣言により、ガイドラインを捕足。
- 1992年 情報伝達の安全に関するガイドラインの発表。

プライバシー、セキュリティ問題について、OECD事務局において、1992、1994、1996年にミーティングをもち、報告書が公表されている。

今後、OECD理事会が、電子情報伝達の暗号化に関する勧告を1997年にだす予定である。

(1) ICCPとして今後取り組む課題

第1にEU指令の第三国への情報移転に関する問題。

第2にニューテクノロジーとプライバシーに関する問題。新しい技術がプライバシーにどのようなリスクをもたらすのか。あるいは新しい技術をどのように対応することによって、このリスクが拡大したり縮小したりするのか。

高速道路利用における個人情報を例としたビデオの技術、すなわち監視テクノロジーという問題。

電子商取引；暗号化に関する問題

本人確認に関する問題

安全と消費者保護に関わる問題

(2) ICCPの今後の活動計画

1997年11月21日 フィンランド 「電子商取引の国際化」をテーマ。

1998年4～5月 カナダで「電子商取引の国際化」のフォロー。「消費者保護」「プライバシー」「セキュリティ」「二重課税」がテーマの予定。

(3) CCPの今後の活動計画

日時；1997年3月3日～4日

場所；パリ

会議名；国際フォーラム「Gateways to the Global Market :Consumers and Electronic Commerce」

消費者保護並びに安全および暗号化について、その政策がどのようにあるべきなのか、技術関係のもとでどのような問題が発生しうるのか、又、将来においてどのような問題が発生するのかという問題を議論する。

4.1.3 調査内容

4.1.3.1 E U指令について（1995年10月の個人情報保護に関するE U指令）

O E C Dとしては、検討を始めたところである。現状は以下の通りである。

E Uが単一市場化を目標としており、E U諸国においては、個人情報保護について既存の法律もあり、E U指令が期限とする1998年10月までの法整備は難しいものではないと思われる。

しかしながら、E U域外諸国に関する問題がある。第三国問題に関しては、多国間関係の検討はそれほど進んでいない。E Uとアメリカ、日本、カナダ、オーストラリアのように二国間での非公式な関係（接触）は進んでいる。

4.1.3.2 各国の状況

O E C D加盟国メンバーにおいて、E Uディレクティブに対する動きは、以下の通りである。

(1) E Uメンバー諸国

イタリア、ギリシャ

両国とも、1995年10月のE U指令の段階では、プライバシーに関する法律はなかった。1998年10月24日までに各国で法律を作ることが要求されているので、2国にとっては大きな問題となるが、全くないところから作る方が、既存のものを改定するよりも容易かもしれない。

イタリアは、1996年12月に議会にパーソナルプロテクションの関する法律を提出した。

ギリシャは、1996年12月までに議会に法案を出す予定であった。

ドイツ

既存のパーソナルデータプロテクション法は、強力なものなので、むしろE U指令に従うことは、もっと下げる必要があるのか、という議論になっている。

オーストリア

高いレベルの法律が出来ているので、E U指令に合わせるために今の法律の構成を変えることは考えられていない。

イギリス

1984年のデータプロテクション法は、EU指令と少しずれがあるようなので、今後検討していく予定。内務省のコンサルテーションペーパーにより、一般の人からも質問や意見交換をしながら、どういうふうに変更したらよいか提言を考えている。また、個人の持っているIDカードの管理の問題が議論されている。

ベルギー

EU指令にそった形で法律を改正していく。

オランダ

パーソナルレジストレーション法をEU指令に適合するように、パーソナルデータプロセッシング法と範囲を変えて、新しい法律に変更する。

フランス

国務省で検討中。

デンマーク

EU指令で要求しているのは、民間部門と公共部門の両方に適用される法律であるが、現在は別々のものであるので、これから検討していく。今後の予定では、今年の7月頃新しいものを提案して、議会にかける。

スウェーデン

1972年のデータプロテクション法はあるが、現状ではかなり古いものになっているのでEU指令に適合するような改正を考えている。

(2) EU域外諸国

オーストラリア

委員会が出来て、総合的なプライバシー法を制定した方がよいと提言。これを受けて、1995年12月に政府が新しい法を作るときには、民間と消費者等にも意見を聞くということで進めている。

カナダ

OECD勧告後、1984年プライバシー法が出来たが、主に公共部門を対象としており、民間部門は対象になっていない。カナダは連邦法以外にも、州法があり、ケベック州は、新しく民間部門を含む法律を作っている。州毎の取り決めであるが、1996年カナディアン・スタンダード・アソシエーション(CSA)が、個人情報保護に関するモデルコードを作った。

アメリカ

総合的ではなく、セクター毎に保護する形をとっている。EUの立場とは異なる。Information Infrastructure Task Force(95.6)にNIIとPrincipal for Providing and Using Personal Information というものを公表した。それを受けて、法務省が1995年10月に「ホワイトペーパー プライバシーアンドNII」をだした。コンシューマープロテクションビューローがプライバシー保護よりもプライバシープリンシプルのプリンシプalsを消費者保護にも適用しようと検討している。

4.1.3.3 質疑応答

- (1) モールを構築する側からみて、プライバシーを保護するために検討されていることはあるか。

まだ検討はない。むしろ、リアビリティに関するのではないか。断片的に取扱ってきているが、全体的視野に立って、電子商取引の問題を最近検討しはじめたところである。電子商取引の分野でどのようなことがなさなければならないかということを取り組んでいる。

- (2) 諸外国において、プライバシー保護についてある一定レベル以上に達している事業者にマークを付与している国、あるいは検討している国はあるか。

政府関係がマークを付与するということは知らないが、民間の団体がマークを出すということを考えているようである。

- (3) モールやネットワーク事業者に対して、プライバシー保護、セキュリティ面でどこまでのレベルを必要とするのか。又、個人情報保護については、暗号化したデータでの伝達の義務化等を検討しているか。

電子商取引のためのプライバシーに関する保護のためのガイドラインは検討していない。現在暗号化政策を検討しているが、暗号は個人情報保護の上では重要であるが、電子商取引の個人情報保護のために暗号を使用することまでは考えていない。

- (4) 電子商取引における国際間取引において、プライバシーの侵害が生じた場合を想定して、国際的な救済機関の設立の検討はありうるか。

消費者政策の中で、国際間取引における消費者を救済するガイドラインは必要と考えるが、具体的な検討はこれからである。

- (5) 電子マネー・電子決済の検討状況について。

民間部門における問題としては何があるかを、消費者からの観点で検討することに

なっている。電子マネー・決済については、OECDの多くの部局で検討されている。

第一に、銀行組織に関する問題の中で、財政問題を取扱う部局が、電子マネーに関してG10の大蔵省と中央銀行の代表者のグループを作って、検討している。

第二に財政的な問題に対するアクションタスクフォースの部局が、新しいテクノロジーが電子取引におけるリスクを作り出すのかどうかということを検討している。

第三に国家財政に関する部局が、税金支払・徴収にかかる問題を検討している。

第四にマクロ経済的な分析の中で、電子マネーはマネーサプライのコントロールにどのような影響を及ぼすか。

第五に、プライバシーに関する問題で、技術的に匿名性を確保できるかどうか。

4.2 European Union(EU)

4.2.1 組織の概要；

European Union(EU、欧州連合)は、1967年に創設されたヨーロッパ共同体(EC、European Community)を前身としている。欧州の域内の統合を目指す欧州連合条約(Treaty on European Union、マ-ストリヒト条約と呼ばれている)が、1993年11月1日に発行したことを受けて発足した。現在、加盟国は12カ国となっている。

EUは欧州委員会、閣僚理事会、欧州議会、欧州裁判所の4機関が中心となっている。

EUは長い間プライバシー問題に積極的に取り組んでおり、1981年には、ヨーロッパ評議会の協定を批准するよう、その加盟国に対して勧告している。

- 訪問先住所；107,avenue de Cortenbergh B-1040 Brussels BERGIUM
- 訪問日時；1997年2月11日(火)10時~12時
- 対応者；European Commission, Directorate General (欧州委員会)
 - ・ Christine SOTTOG-MICAS
 - ・ Nick Platten

- 訪問目的

1995年10月24日に採択された「個人データ処理に係る個人の保護及び当該データの自

由な移動に関するの欧州議会及び理事会の指令」に対するEU加盟各国の対応状況と、特に第三国へのデータ移転（第25条）及び第25条の適用制約（第26条）に関するEU委員会の見解について調査する。

4.2.2 調査内容

4.2.2.1 EU加盟諸国のEU指令への対応状況

(1) イタリア、ギリシャ

両国とも過去にプライバシー保護法がなかったため、EU指令に対応するため法案の整備を進めている。

イタリアについては、1996年12月に法案が提出され成案した。

ギリシャも、1996年12月に法案が準備され議会に提出された模様である。その後1～2カ月以内に成立する見込みである。

(2) オランダ

既存の法律（1988年制定の個人データ保護法）はデータファイルを対象としている。一方、EU指令は個人のデータおよびそのデータ処理を対象としているところから、これらの点の相違を埋めるために改正を検討している。

(3) ベルギー、スウェーデン

ベルギー（1992年、個人データの処理に係るプライバシーの保護に関する法律）、スウェーデン（1973年、データ法）等、法律を制定しているが、EU指令に対応するため、改正の準備を進めている。

(4) デンマーク

既存の法律（1978年制定のデータファイルに関する法律）は、公的部門と民間部門が別になっている、いわゆるセグメント（個別）方式である。そのため、この方式の違いも含めて対応を検討している。

(5) 英国

既存の法律（1984年制定のデータ保護法）をEU指令に適合させるための手続きとして、内務省のData Protection Sectionは、1996年3月に「コンサルテーションペーパー（Consultation Paper）」を作成した。これは、EU指令に対する英国の対応に関し、民間企業等主要部門からの意見を収集するためのものである。意見は1996年7月19日までに回収され、この意見を受けて現在改定案を準備中であ

る。今年5～6月に議会に提出する予定である。

(6) ドイツ

西ドイツ時代の1977年制定の連邦データ保護法(1990年に改正)は、EU指令よりも厳しい内容となっている部分がある。そのために、国内の保護法を緩和すべきかどうかを含めた議論がなされている。公的部門と民間部門の法律が異なる点についても検討している。

(7) フランス

プライバシー保護法(データ処理、データファイルおよび個人の諸自由に関する法律)は1978年に制定され、法律の規定の順守を監督する機関としてC N I L (Commission Nationale de l'Informatique et des Libertés: 情報処理と諸自由に関する国家委員会)が設けられている。その後雇用問題を反映して1992年に法律が改正されている。EU指令に関しては、国務院において、法律への反映を検討している。

4.2.2.2 EU指令の第三国条項の解釈

わが国をはじめとするEU域外の第三国から見た場合、同指令のポイントは、第25条に規定されている「第三国への個人データへの移転」と、第25条の適用制約を規定している第26条に関するものである。

EU指令第25条は、第三国への個人情報の移転について、当該第三国が個人情報に関して十分なレベルの保護を確保している場合に限って行なうことができると規定している。

4.2.2.3 電子商取引との関連

今後普及が見込まれる電子商取引とデータ保護を中心に意見を聴取した。

- ・現在は電子商取引において個人データがどのように扱われるのかといった問題を調査している段階である。これを分析して標準化することが必要である。
- ・各国にライアビリティ(責任)の問題があると考える。
- ・オンライン上でショッピングをする際にはアクセスした履歴が残り、それを第三者に通知したり個人データのみを抽出できるソフトがあり、店頭で購入した場合と同様に購入歴が残らないような技術的なしくみが必要である。
- ・インターネットは広報・電話・手紙の要素がある。

- ・電子商取引とプライバシーの問題を検討する上で、法律（責任・罰則）、規範（民事訴訟）、技術的（ネットワークを誰がコントロールするか）の3点について検討してゆくことが必要である。
- ・最近活発となっているダイレクトマーケティングそのものが個人データ保護の観点から問題としているのではなく、消費者（個人）が知らないことと知っていたとしても個人データを提供しないことを選択できないことに問題があると考える。

4.3 ドイツ銀行協会 Bundesverband deutscher Banken(BdB)

4.3.1 組織の概要；

1951年に設立された金融機関の共同組織で3大総合銀行、152の地方銀行、59の個人銀行家が中心で、加盟数は303金融機関となっている。

- 訪問先住所； Kattenbug 1 50667 Koln GERMANY
- 訪問日時； 1997年2月12日（水）14時～16時
- 対応者； Wulf Hartmann
- 訪問目的

個人データが最も厳格に保護されている国の一つのドイツの金融機関が個人データに関して実務上どのような取扱を行っているかについて調査する。

4.3.2 調査内容

4.3.2.1 ドイツの金融機関における個人データ保護のしくみ（概要）

(1) 金融機関における個人データ保護

法律としては、ドイツ基本法（1983年）の第2章 人格権で規定されている。

連邦データ保護法は、一般的、抽象的な法律である。

民間部門は、22条～32条、33条～35条、36条～38条で規定されており、刑罰についても触れられている。

契約においては、約款（General business Conditions）の一部に「銀行機密」条項がある。これは、独自につくったコンセプトで、法律が作成される以前から存在したものである。

(2) データ処理の適法化の条件

法律による認定

データ（顧客）主体の同意を得ること。

(3) データ主体の権利

- ・通知をうける権利
- ・アクセス権
- ・訂正・削除権

(4) 監督制度

公的部門

- ・連邦データ保護監督官
- ・州政府の監督官庁

民間部門

- ・州政府の監督官庁は、事前にデータ処理をコントロールする権利を有する。
法技術的な問題については敏感で、その場合は銀行協会への連絡がある。
使用者が従業員の中から任命する企業内のデータ保護受託者の地位について、法的保護と州政府による解任制度がある。
- ・検察官は、事後的な救済を行うが、事前のコントロールで解決できるので刑事裁判になることは少ない。

(例) 銀行員が住宅ローンに関する情報を保険会社に提供して、保険会社が住宅に関する保険のセールスに使用した場合で、罰金刑となった。

- ・守秘義務は、一般的には法律として規定されていないが、税法と民事訴訟法に一部の規定がある。

民事訴訟法で、銀行員が証人になった場合に守秘義務（証言拒否）がある。

銀行に対して税の関係の家宅捜索がなされた場合に顧客のデータを捜査されたことがある。私法における個人データ保護と公法における個人データ保護は別と考えるべきであるかもしれない。

4.3.2.2 電子化と連邦データ保護法

1996年12月にマルチメディア法案（正式名：情報・コミュニケーション法案）の

一環でテレサービスにかかるデ - タ保護法が閣議決定された。この内容は、一般の連邦データ法の抽象性を排除したもので、特別法として位置付けられる。

金融機関の業務では、ホームバンキング、インターネットバンキング、プロバイダーを介したオンラインバンキングが関係する。

現在、意見書を取りまとめ中で、銀行の特殊性が盛り込まれていないとの理由で反対の立場をとっている。

- ・ デ - タ処理の合法性についてテレバンキング（顧客から銀行にデ - タを電子的に送ることによって取引を行うことで、電話で音声を通じて行うものは含まない）のみについて規定しているが金融機関としては銀行業務全体に対して行いたい。
- ・ 匿名で送金することを求めているが、これは銀行業務の基本的な性格に反している。
- ・ 一般の連邦データ法との間で連携を図るべきである。

4.3.2.3 E U指令と連邦デ - タ保護法

(1) 金融機関の連邦デ - タ保護法への過去の対応

1978年の制定時は情報技術開発の過程で法律の裏付けが必要となっており、経済界と一般市民の双方にメリットがあることから賛成をした。但し、事務処理が簡素にできるようにすべきであるとの意見を加えた。

1990年の改正時は銀行業務には支障がないのであえて意見を付さなかった。

(2) E U指令に関連する連邦デ - タ保護法の論議

既に内務省との間で何回も接触をしており、5つの金融関係団体が合同して組織している中央金融委員会名で1996年7月に意見書を提出している。

(3) E U指令の個々の条項についてのコメント

全体

「データ処理の目的に合う」の解釈が厳しくなることによって、承諾書を数多く徴求する必要が生ずるかもしれない。例えば、有価証券をとりかわした際のデータを普通預金のセールスに使用することが目的にかなうかどうかの問題となる。

第1条 指令の目的

対象データの範囲は現行ドイツ法よりも、E U指令の方が大きい。

非自動処理についても自動処理と同様な取扱が要請されるかもしれない。

第8条 特別カテゴリーのデータ処理

特別カテゴリーデータに対する規定ではデータ主体の明確な同意を要求しているが、例えば送金において相手の名前が政党名で、摘要欄に政治資金とした場合に問題となる可能性がある。これは、1.普通預金の開設時に了解書を徴求する 2.送金目的を記載するように顧客に依頼するという対応があり、監督官庁がいずれかの方法を行うように指示する余地は残っているが、金融機関としては、決済の迅速性、機能性の観点から、振込み自体に明確な同意が含まれると解釈したい。

第 11 条 データが、データの対象者から収集されなかった場合の情報、第 12 条 アクセス権

収集時の情報提供義務については、送金の場合に送金先に個人情報が伝達することのように明らかに顧客に知っている情報を通知する必要はないと考える。つまり、必要以上に知らせる必要はない。したがって、ドイツ法では何が必要であるかについての規則が必要である。

第 15 条 個人に関する自動的判断

ドイツ法にとっては全く新しい概念である。

どの条項が銀行業務に関連するかの解釈が必要である。この規定はおそらくクレジットスコアリング（ランク付け）の問題であるように思う。すなわち、与信判断の最終判断は人間が行っていることが必要である。仮に、完全自動化するシステムを構築した場合には、苦情処理する部署が必要で、それは人間が対応しなければならない。

第 25 条 第三国に対する個人データの移動の原則、第 26 条 第三国に対する個人データの移動の免除

第 25 条の規定は厳しいもので、この条項がデータ保護レベルの平均化を目的とし、同等な保護レベルが必要であると解釈すると、EU内の通貨統合参加国と他の国の間に壁をつくるものとなり、金融機関の業務に支障が生ずる。

しかし、第 26 条はかなり多くの例外規定を設けており、第 1 項 a)ではデータ主体の明確な同意があれば保護レベルが低いと認定された国へのデータの移転も可能としている。

金融機関の業務にあてはめると、送金は契約義務の履行として考え、承諾書は徴求しないと考えており、仮にそれは認められない場合に承諾書を徴求することもさほど困難ではないかもしれないが、ドイツの銀行がインドの会社にデータ処理を外

部委託するといった場合には、問題の解決が難しくなる。外部委託は金融機関以外でも広く行われており、同様に行っていきたい。

第 25 条の「職業上のル - ル」の解釈は医師や弁護士のように法律化された職業についての守秘義務であり、金融界や一般産業界のガイドラインはこれに当たらない。それらはむしろ第 27 条の問題としてとらえるべきものである。

第 26 条 1 項の明確な同意は「疑いなく (without any doubt)」と解釈する。

第 28 条 監視機関

ドイツでは民間部門に対しては地方分権をしており、事前審査は州のデータ保護監督官庁が行い、事後的には検察官の関与を含めて司法的救済を得ることができるようになっており、これは E U 指令の範囲内のものであると考ええる。

4.3.2.4 グル - プ (コンツエルン) 内でのデ - タの相互利用

ドイツの金融機関はユニバ - サルバンク (総合金融機関) の制度をとっており、以前は 1 つの会社でさまざまな業務 (銀行・証券・保険等) を行っていたが、最近では分社化を行い現在ではそれぞれの業務を異なった会社で行っている。

この場合に、別法人になることでデータ主体の同意があってはじめて情報の移転が可能となることになる。したがって、それぞれの会社間でデ - タを共有する場合は、ドイツの金融機関ではデ - タを共有するために承諾書を徴求することになっている。ドイツでは顧客はグループ内でもどこへ情報が流れるかについて知る権利があると考えられている。

この書式については各州政府の監督官庁へ了解をとる作業を行っているが、州が多いこと (16 州) などが影響して 3 年余りの間、協議を続けている。

金融機関としてはできるだけ多くの事を 1 つの承諾書で行いたいが、州の監督官庁はできるだけ狭くしたいと考えている。具体的には住所・氏名と附帯的事項として永遠に続けられるような書式としている。

4.4 The Data Protection Registrar

4.4.1 訪問先概要 ;

1984年に制定された「データ保護法」の執行機関として設置された機関で登録簿への登録、監督（強制処分通知、登録抹消通知、移転禁止通知）、議会宛の年次報告書の提出を主な任務としている。

- 訪問先住所；Wycliff House Water Lane Wilmslow Cheshire SK 5AF
- 訪問日時；1997年2月13日（木）14時10分～16時20分
- 対応者；
 - ・ Elizabeth France；The Data Protection Registrar
 - ・ Rosemary Jay；Legal Adviser
 - ・ David Smith；Assistant Registrar
 - ・ Anne Hinde；Senior Policy Adviser
 - ・ Gill Hoodless；International Officer

- 訪問目的

英国のデータ保護登録官制度及び1995年10月に採択された「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（EU指令）を受けて検討されているデータ保護法(Data Protection Act 1984)の改訂状況について、調査を行う。

4.4.2 調査内容

4.4.2.1 データ保護法(Data Protection Act 1984)

(1) 目的

- ・ コンピュータへの信用度を確立。
- ・ CE（欧州評議会）のメンバー国として条約を批准。
- ・ コードオブプラクティスを確立する。

(2) 個人情報の使用者の義務

- ・ データ保護8原則の標準を設定（公正・合法・利用・正確・適切な量・保有期間・個人の権利・安全）し、履行する。
- ・ 登録簿への登録を義務づける。個人情報の取扱者が、登録していない場合は最高5千ポンド（約100万円）の罰金が課せられる。
- ・ データ主体へ個人データ処理の詳細を明確にする。

(3) 監督制度

8原則を遵守しない使用者へ通知するが、使用者は弁明の機会が与えられる。

国民は次の3つの権利を有している。

- ・ 自己の情報にアクセスする権利。
- ・ 誤った情報に対して、削除あるいは訂正を要求する権利。
- ・ 不正確な情報により損害を被り、法廷で証明した場合に賠償を受ける権利。

4.4.2.2 EU 指令について

- ・ 1995年10月のEU指令に対するハーモナイゼーションに合意。

1998年10月までに英国は、既存のデータ保護法を修正するか新しい法律を制定しなければならない。

英国のデータプロテクション法とEU指令は、おおよそ共通しているが、メンバー国以外へのデータの移転について新しい概念もある。

この点について、今の段階では、メンバー国内での調整も明確でなく、また、データについて適切な保護が得られるなら、第三国へ移転しても構わないということも明確ではない。

- ・ 例外的には、当事者の契約によって決めなければならないということである。

(1) 25条 第三国に対する個人データの移動の原則について

メンバー国以外へのデータの移転の可否はケースバイケースになるだろう。

適切な保護をもつということはどういう事を意味するのか、その解釈について討議中である。

(2) 29条 個人データの処理に対しての個人の保護に関する作業部会について

適切な保護を持たない国とどのように解決すれば上手くいくのか。

それぞれのデータプロテクションの関係者と話をしている。しかしながら、今のところ明確な回答はない。

解釈について、1つだけ明確なことは、データプロテクションに関する適切な法が必要であるということである。

4.4.2.3 データの主体からの苦情について

(1) 苦情の状況

昨年度、約 3 千件の苦情があった。その中で最も多いのは、クレジットの信用度(評価)に関する苦情である。かつては、ジャンクメールのようなDMについての苦情が多かった。

問題が発生した場合、ユーザーとレジストラの間で話し合いが持たれる。裁判所には実際 6～7 件しか持ち込まれていない。

インターネットや電子商取引での苦情はないが、苦情は電子メールについてが大半である。例としては、ある企業に勤めている従業員が会社のパソコンを使って、私的に電子メールを使用する。勤務先を代えたところ、元の勤務していた企業のコンピュータにその個人の電子メールが送られ、会社がそれを見るという苦情である。個人が前の雇用主が自分の電子メールを勝手に見たということで訴えるか、雇用主が会社のコンピュータを私用に使ったということで訴えるのか、どちらのケースもある。

(2) 苦情処理

レジストラは、一般の国民から苦情があった場合に対処する。自動的に処理をしたデータに関わるデータの使用者は、8 原則を履行し、The Data Protection Registrar に登録し、データの使用内容について報告をする。

データの収集にあたって標準的な取扱いをするが、標準的な取扱いをしないで、且つ使用者が The Data Protection Registrar に登録していない場合には、最高 5 千ポンドの罰金が課せられる。

規則を遵守しないものに対しては勧告することができる。

レジストラは、あくまでも苦情の事実を調査するのであって、苦情申立人の代理人になるわけではない。

国民は 3 つの権利を有する。

自己の情報に対してアクセスできる権利。

誤りの情報を削除あるいは訂正を要求する権利。

不正確な情報により損害を被った場合、裁判で訴訟を起こす権利。

それぞれの国で法律が違うので、それを破った場合の法的執行力の方法が違っている。アメリカでは、大半が民間で訴訟を起こして処理している。イギリスであれば、レジストラがアクションを起こすことになる。

業界のアウトサイダーからの個人情報の漏えいにたいしては、レジストラの法的

執行力は、苦情が正当であれば、法律にかけるということであり、当然それは登録している企業に対してである。登録していない企業に対しては、まず登録していないことに対して起訴し、登録した後、苦情の正当性について、捜査することが出来る。

(3) レジストラの体制について

レジストラの職員は政策、法律、マーケティング、広告等いろいろな分野に分かれて約 100 人いる。それ以外に必要なに応じて、契約によりパートタイマーが全国に散らばっている。又、必要なに応じて従事する調査官が全国で 12 名いる。大半は、逮捕する前に通知する事項や法律に詳しいことから、元警察官である。本体に常勤する調査官が 3 名いる。苦情部門では、12 名の職員がいる。

現在のスタッフで十分であるが、今後は国際的な苦情が増えることが予想される。

4.4.2.4 質疑応答

(1) どの国が適切な保護レベルに達していないと思われるか。日本はどうか。

他の国も興味はあるようだけれども、まだ分からない。

(2) 1984年のデータ保護法は、電子商取引を特に念頭においているか。

消費者保護、商取引における資金移動、機密性、二者間の同意については関わりがあり、広い範囲で商取引の分野のデータ保護に関わるものである。

(3) ネットワーク上で個人情報盗まれることを調査するケースを想定しているか。

盗まれるということは、ハッキングということと、情報についてアクセスする権利のある人が、取り出して悪用するという2つのケースが考えられる。個人情報を所有するのはいいが、そういう情報を使って多くの分野で使用することは違法である。それについての捜査権は、レジストラにある。但し、イギリスにおける捜査権しかなく、インターネットにおいて国際間での問題の場合は、困難である。

(4) 日本で考えているマーク付与制度について、どう思うか。

現在イギリスでは、マーク付与はない。ビジネスのプラクティスとして、ISO 9000品質管理にデータ保護を組み込めないかという検討がある。又、セキュリティに関しては、機関に登録する義務があり、これ自体に価値がある。英国政府は、セキュリティのスタンダードが出来れば、その監査の実施を考えており、その監査はインフォメーションのレベルによって、自社監査でいいところと、もっと厳しい監査をしなければならないということを検討している。

(5) ISOのような標準化をプライバシーについても考えられるか。

カナダは自国内の個人情報に関するスタンダードを作った。ISOに持ち込み、国際的なスタンダードになりうるのか問い合わせているが、まだ回答はされていない。もし、カナダの標準が、国際的な標準となってくるとすれば、問題としては、データの移転における受ける国の適切な保護があるかどうかの標準ということになってくるだろう。それによって、国際的なコードが作られるのではないか。国際的に標準化したものであれば、OECDのガイドラインがある。

4.4.3 電子商取引との関連

ECOMの電子商取引におけるプライバシー保護の考え方は、商業をベースとした企業間でのEDIに関する分析とそれに対するプロトコルを念頭においたイギリスの考え方とベースが異なるものである。

商取引における個人のプライバシー等を守るため、どのようにして商取引間における安全な環境を作り上げるかという新しい分野についての考え方である。

インターネットでは、個人情報の収集の方法に関心がある。現在、インターネットサイティに、消費者のコンピューター上のアドレスについて、個人名が登録されているけれども、その名前の後にプライバシーマーカというものを作って、そこに何を入れてもよく、消費者の意思が明確に出せるスペースを作るということを提案している。ダイレクトメール等が送られて欲しくない場合に、その意思表示を明確に表現できるものである。

4.5 英国内務省 Home office (Data Protection Section)

4.5.1 組織の概要；

英国の内務省で治安、警察、消防等を担当しており、個人データ保護に関しては法律の制定・改訂を担当している。

- 訪問先住所； Room 1181 Home Office Queen Ann's Gate London SW1H
- 訪問日時； 1997年2月14日(火) 14時～16時
- 対応者； Graham Sutton

Constitutional and Community Policy Directorate Liquor, Gambling and Data Protection Unit

- 訪問目的

英国の個人データ保護制度及び1995年10月に採択された「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」(EU指令)を受けて検討されているデータ保護法(Data Protection Act 1984)の改訂状況について、調査を行う。

4.5.2 調査内容

4.5.2.1 データ保護法(Data Protection Act 1984)の改訂スケジュール

1995年10月24日	EU指令採択
1996年3月	コンサルティングペーパー 発表
1996年7月	コンサルティングペーパー 回答(約300社)
1996年12月	コンサルティングペーパー まとめ・分析
1997年2月現在	改訂のための法案を提出するための準備作業
1997年秋	議会で改訂案を提出
1998年4月	発布
1998年10月	実施

現政権の予定であり1997年5月予定の選挙で政権交代すれば変更の可能性有。

4.5.2.2 EU指令の第三国条項に対する考え方

(1) 英国政府の基本的スタンス

海外にデータを送ることを困難にしない。

英国のデータ使用者の負担をミニマムにしたい。EU指令は原則であり、そのまわりには多様なものが存在すると思われる。

(2) 第25条 第3国に対する個人データの移動について

解釈するに当たり、以下の点で明確ではなく、英国も含めEU各国は国内法化する場合に苦労している。

適切な保護レベルかどうかを誰がどのような手続で判断するのか。(EU・各国・使用者)

適切な保護レベルとは何か(法律・行政規則・自主規範・慣習)

なお、適切な保護レベルかどうかは一義的には使用者(ビジネス)が判断するべきであり、それに対してデータ保護登録官、EU委員会が監視することができる権限を

有する。

また、適切な保護レベルは移転するデータの種類、目的、移転先の国・業種・当該会社によって異なり、あくまでケースバイケースで考えるべきである。その際には第三国の一般法・特別法等すべてを考慮すべきである。なお、法律は、あれば適切な保護レベルではなく、どのように執行されているかが重要である。

(3) 英国政府が考えている手続き

使用者は、セントラルポイントが定めた基準（全ての種類データの移転が可能な国、又は特定のデータを特定の目的で移転することができる国）によって、個人データを移転することができない場合には、移転先の国、業種、当該会社における個人データの保護レベルを勘案して、移転するデータが第三国において適切に保護されるかどうかを判断し、保護されると判断をした場合は、その責任において移転を行うこととしたい。

データ保護登録官は苦情が出た場合等において必要に応じて調査し、上記の判断が適切かどうかについてチェックをする。（データ保護登録官はその権限を保有する。）その際には第三国の一般法・特別法等を勘案して判断する。

第三国の保護レベルが適切でないと判断した場合は移転を中止させるか、または自主規範を変更させる。

EU委員会はデータ保護登録官が見逃したり、その判断が誤っていると考えた場合は介入することができる。

(4) セントラルポイントの役割

セントラルポイントは内務省又はデータ保護登録官が担う。

使用者(ビジネス)が判断した個人データの第三国移転に対する事後的チェック。

自主規範における個人データの第三国移転に関する事項に対する助言、監督。

（イ.全ての種類データの移転が可能な国、又はロ.特定のデータを特定の目的で移転することができる国）の基準を定め、使用者（ビジネス）に提供する。

(5) 第26条 第3国に対する個人データの移動の免除に関する英国政府の解釈

EU指令第26条1項でデータ主体の明確な同意がある場合は保護レベルの低い国への移転も可能となるが、ここで言う「明確な同意」は十分に表現する（explicit）と解釈すべきであり、必ずしも「文書化」は意味しない。但し、医療機関において待合室の壁にかかげるだけのように見たかもしれないし、見ていないかもしれないような

場合はこれに当たらないであろう。

4.6 カナダ産業省 Industry Canada

4.6.1 組織の概要

カナダ産業省は、カナダ政府における国家の経済問題に関して責任を持つ重要な省である。日本における通産省に相当する。世界的な統合、及び、知識集約型の経済成長に特徴付けられる世界において、カナダにおける職業の増進や発展を促すために設立された。主な機能は、政策の勧告、産業部門の情報の提供や公共事業の実施である。カナダ産業省は、効率的で、競争的で、協力的で、公平で、かつ、告知されている消費者により引っ張られる市場を作ることである。また、カナダの産業界に対して、国内外の機会を利用し、科学的、即ち、技術的な進歩に専心できるよう奨励する役目を追っている。

- 訪問先住所； 300 Slater Street , Room 2080D Ottawa Ontario K1A1C8

- 訪問日時； 1997年2月17日（月）10時～12時

- 対応者；

(1) Industry Canada

Stephanie Perrin

Arthur Cordell

Edith Core

Serge Presseau

Charles Chenard

Pierre Leduc

Prabir Neogi

Denis C.Kratchanov

(2) Department of Justice Canada

Heather H.Black

E.Michael Power

- 訪問目的

1995年10月に採択された「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（EU指令）を受けた各国の国内法の整備

状況とカナダ産業省における個人データ保護に関する活動状況を調査する。

4.6.2 トピック

カナダは、日本のように国としての組織整備がされておらず、これから1年かけて整備をしていく予定である。

カナダ政府が主体となって、コマースネットカナダを設立予定であり、日本のE C O Mのような組織をカナダとして設立する予定とのことである。

4.6.3 調査内容

4.6.3.1 カナダ政府としての最近の動向

政府としてのプライバシーに関する課題は、1994年、大臣への諮問委員会への最終報告書としてまとめた。プライバシー、セキュリティに関する特別なページがある。

1998年までに、政府関連のサービス（税金関係等）を電子的に行なうこと、また、政府が集めた個人情報に関する保護法の適応を民間部門に広げることについて考えている。

1990年、E U指令案がでたため、カナダ規格協会（以下、C S A）で民間部門における個人情報の保護に関する規格を制定し、プライバシー問題について取り組んできた。

海外の商活動を含め、C S Aの統一規格で活動が行なえるよう、法務大臣、及び、産業大臣に法律を整備するよう指示がなされた。そのため、法務省では、それらの法律の整備を行なっている。

カナダ規格に基いて法を作るように指示があった理由は、I S O 9 0 0 0に認定してもらいたいためである。

I S Oではカナダの基準に基いて検討を行ない基準案を作り、検討委員会を新たに設置し継続検討することとなった。また、あまり意識をしていないI S Oの参加者に対しては、カナダ政府は、教育する側の立場にいる。

法律の整備が進む前に民間部門が先に進んでいる。しかし、基準に従っていれば、O Kというようにしていきたい。

会計事務所で監査を行なうことや、W T Oにかけることも考えている。

政府機関と民間部門が情報交換する方法として、公開鍵方式を用いた試験システムを検討している。法務省、産業省で行なっている。技術的な試験を、約4週間後に開始する予定である。

1994年、カナダの主な州、モントリオール州、ケベック州等の弁護士が集まって、著作権に関する問題を検討した。子どものポルノ等の微妙な問題について討議を行なった。

4.6.3.2 質疑応答

- (1) プライバシー保護に関する、カナダの規格をISO9000に認証してもらいたいのか、カナダの法をISO9000にあったものに作りたいのか。

カナダの規格を、ISO9000で認証してもらいたい。世界中で、いかなる国において商活動を行なっても、その規格に合うよう製品開発等の商活動を行なっている限り、世界中で認められることになると考えるからである。

- (2) プライバシーの保護について、会計事務所で監査を行なうことを考えているが、監査は民間部門で行なうということか。

現在は、民間部門で行なっている。

- (3) 政府は、規制をするようなことを考えているのか。

政府としては、最初から規制を行なうことを考えているのではなく、問題が発生すれば政府が介入できるような法律の整備を考えている。ただし、政府としては、あまり金のかからない方法で、かつ、民間部門で行ないたいと考えている。

- (4) 監査企業は、大手6社に限るのか。

会計事務所の大手6社以外にも、会計監査が行なえる会社であれば、どこでも可能と考えている。小企業から、国際的な大企業までであるため、3レベルを考えている。

1つ目は、CSAの規格に合致していると自己宣言している企業レベル、2つ目は、CSAに承認してもらっている企業レベル、3つ目は、ISOの承認をもらっている企業レベルである。

- (5) CSAの承認とは、どういう意味か。

CSAの承認済みのマークとして、JISマークのようなことを考えている。

実際に事例がないため、まだ、CSAも検討中である。ISOに登録する場合は、金がかかるため、CSAの場合は、そのようなことは考えていない。

自己宣言レベルは、自社内で単に宣言するレベルと考えており、第三者からの承認は考えていない。

- (6) 監査に関する公式文書はあるか。

この監査は、任意で、企業にとって金がかからず、かつ、消費者が認めてくれるも

のを考えている。問題を起こした企業と、そうでない企業を区別するためのものと考えている。

- (7) 日本では、プライバシーに関するガイドラインを作成し、マークの付与を考えている。

C S Aでは、第3者に委託する苦情処理方法も検討している。特に、法律が民間で、カナダの州レベルで遵守されるためには、その法律が制定される必要がある。

- (8) 現在、日本では、法規制の実施は難しい状況である。カナダでは、法規制が可能なのか。

カナダでも法規制の実施は難しい。別の方法として、カナダの銀行協会がC S Aに合わせてモデル規格を策定した。また、大蔵省ではC S Aの規格に合わなければならないという規則を作ったが、銀行業界では自主規制してきているため、その規則の実効的な影響は無い。

- (9) カナダにおいて、ネットワーク上で創設された、仮想商店街、仮想店舗等についての問題点を、プライバシー問題も含めて、どの程度把握されているか。

カナダでは、ダイレクトマーケティング協会があり、C S Aの基準に合うよう電子商取引に関する倫理基準を作ろうと考えている。

- (10) ネットワーク上における、ショップの集合体であるモールに関する約款があるか。また、ある場合、その約款が守られなかった場合の法的な措置は考えているか。

そのような問題は、カナダでは市民権に関する問題で、州の管轄であり、連邦政府は対応を考えていない。また、現時点では、どの州も、そのような法を作成したと聞いていない。それらは、すべて契約法に関するものである。

4.7 アメリカ Executive Office of the President Office of Management and Budget

4.7.1 組織の概要

Office of management and Budget (行政管理予算局 O M B) は、大統領行政府の一部であり、ワシントン D.C.においてホワイトハウス (White House) の下に位置していて、データ保護等のポリシーに関しても策定する。 O M B には、 5 5 0 人程度の専門家とサポートスタッフがいる。

- 訪問先住所 ; New Executive Office Building, Room 9026 725 17th Street, NW Washington, D.C. 20503

- 訪問日時 ; 1 9 9 7 2 月 1 8 日 (火) 1 0 時 ~ 1 1 時 3 0 分

- 対応者 ;

- (1) Office of management and Budget, Information Policy & Technology

- ・ Bruce W. McConnell (CHIEF)

- ・ PETER N. WEISS

- (2) Federal Trade Commission (F T C)

- ・ J. Beekwith Burr

- 訪問目的

1 9 9 5 年 1 0 月 2 4 日に採択された「個人データ処理に係る個人の保護及び当該データの自由な移動に関するの欧州議会及び理事会の指令」 (E U 指令) に対する米国の対応状況について調査する。

4.7.2 調査内容

4.7.2.1 EU 指令への対応

- (1) データ保護に関する法律

E U 指令は、公的部門および民間部門を対象としているが、米国の場合は分野ごとにまたは適時に法律を制定する方法論をとっている。例えば、 1 9 7 4 年に制定したプライバシー法は、公的部門を対象に規定したものである。また、 1 9 8 6 年制定した電子通信プライバシー法では、電気通信事業を営む民間部門の企業等を対象に規定している。更に、民間部門のプライバシーに関しては、この他に個別の法律が存在する。

- ・ 1 9 8 7 年コンピュータ安全保護法

- ・ 1988年ビデオプライバシー保護法
- ・ 1988年コンピュータマッチングプライバシー保護法
- ・ 1991年電話消費者保護法

また、民間部門に関しては、政府はなるべく介入せず、自主的な規制に任せる方向で対応してきた。今後もその方向性は変わらない。

なお、公的部門、民間部門の種々のプライバシーに関する保護法は、1980年のOECDのプライバシー・ガイドラインの原則に準じたものとなっている。

プライバシーに関する世論は、以前は政府が個人の情報を収集することに関して厳しい目を向けていたが、最近ではビジネス分野の活動における個人情報の収集等に対して心配するような傾向にある。このようなことから、民間部門は個人情報に関する取り扱いについて、十分な自主的規制を推し進めていく必要がある。

(2) EU 指令に関する対応

米国は、以上のようなプライバシー保護に対する方向性から、今後も全体を包含するような法律は策定しない。

米国は民間部門に関する個人データの保護については、企業の自主規制を尊重する。

プライバシー保護に係る苦情受付窓口等は特に設けていないが、詐欺等の犯罪に発展するような場合については、Federal Trade Commission (FTC) や各州の司法省が当該法律によって対応する。

(3) その他

日本の通産省が検討しているようなマーク付与の制度は、米国政府としては考えていない。同様なものとしては、民間のアプローチとしてCDT (The Center For Democracy And Technology) やBBB (ベター・ビジネス・ビューロ) が自主規制によるレイティングを考えている。

4.7.2.2 電子商取引との関連

インターネット上での販売は、通信販売の延長と考えている。したがって、通信販売を行っている業界が自主的な規制によって個人の情報を保護する措置を講じなければならない。(米国では、コマースネットによってこれらの問題は検討されている。)ただし、ECにおいて不正な行為が発生した場合には、FTCの所管として対応することになる。

インターネットでは、WWWにアクセスするだけでその人のIPアドレス等が残ること

になり、さらにアンケートや質問に答えるとその情報も個人の情報として収集されることになる。しかしながら、米国においては、このように収集した個人に関する情報は、WWWの運営者がどのように使ってもそれを規制する根拠となるものがない。このような問題に関しても、政府が規制するのではなく民間の自主的な規制に任せることになる。一部の会社（インターネットプロバイダー）では、インターネット上のプライバシー保護に関する方針を定めているところもある。

インターネットプロバイダーのプライバシー保護レベルに関しては、<http://WWW.CDT.ORG> にその情報がリストアップされている。CDTは、通信販売業者等が集まって、人権を守る目的で活動している団体である。

通信販売業者の団体は、ダイレクトメール等を受け取った人が、自身のデータをマーケティング・リストから削除するように要求したとき、これに応ずることを自主的規制で行っている。

インターネット上で最近問題になっているのは、子供から情報を収集することについて、FTCに寄せられる苦情が多くなっていることである。

医療や保険の分野の個人に対する情報の保護措置について、厚生省に対して3年以内に法律を策定するよう指示が出されている。メディカル・インフォメーション・ビューロは、FTCに対してクレジット・ビューロと同様に、消費者からの苦情によって自分の情報をチェックし変更することができるような方法の導入を伝えてきている。

ネットワーク上の詐欺等の行為を調査するのは難しいが、電子通信プライバシー法によって対応することは可能である。

4.8 アメリカ Commerce Net (eTRUST)

4.8.1 組織の概要；

eTRUSTの任務は、電子決済における信頼と信用を確立することにある。

eTRUSTは、プライバシー問題、セキュリティ問題、認証問題等に関するガイドラインを確立し発展させるための基盤を構築することにより電子商取引の拡大を促す役目を担っている。

eTRUSTの最初のプロジェクトは、オンライン上でのプライバシー問題である。eTRUSTは、オンライン上での商取引におけるプライバシー、セキュリティに関する「信

用マーク」、即ち、承認され、かつ、信用のおける記号を作成し、認可する組織である。eTRUST プログラムの究極の信託受益者（利益を享受する者）は、オンライン上のユーザ自身である。その結果、ユーザにとって、詳しい情報に基づく選択がより可能になるのである。

- 訪問先住所；4005 Miranda Ave., Suite 175 Palo Alto CA 94304 USA

- 訪問日時；1997年2月19日（水）10時～12時

- 対応者；eTRUST

- ・ Andrew Boer (eTRUST Product Manager)

- ・ Susan Scott (eTRUST Program)

- 訪問目的

- 1995年10月に採択された「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（EU指令）を受けた各国の国内法の整備状況とコマーシヤルネットにおけるマーク付与方式によるデータ保護の検討状況を調査する。

4.8.2 トピック

信用状と認可されたガイドラインを確立することが現在の活動である。

1996年の第4四半期に、プライバシーに焦点をあてた準備計画を開始した。ビジネスモデルを考え、そのモデルを外部の会計事務に評価してもらっている。1997年の上半期に商業ベースの提案を行なおうと考えている。

4.8.3 調査内容

4.8.3.1 eTRUST の活動

電子商取引は、1994年に覚醒し、1995年に概念の提案がなされ、1996年に問題点が抽出され、そして、1997年に、それらの問題点が解決されれば、市場の拡大が見込まれる。

その問題点とは、電子商取引の市場が拡大するためには、消費者の信頼や信用を確立する必要があるということである。また、1996年10月、セキュリティの欠如とプライバシー問題が、電子商取引が受け入れられない大きな原因であるというレポートが、G I G Aの市場調査結果として発表された。

eTRUST のメンバは、Commerce Net、the Electronic Frontier Foundation(E F F)、設立企業計 11 社である。E F F は、世界中の消費者に幅広く影響を与え、電子媒体上での市民的自由と消費者の権利の擁護者として尊敬されている。

eTRUST の業務は、「trust marks」という記号を使い信頼の基盤を確立すること、保証行為と監視行為、事業者や消費者の意識付けと教育、信頼のガイドラインの確立及び展開のためのオープンな場の提供である。

eTRUST が考えているマークは、以下の 3 種類である。(なお、実際のイメージ図は、eTRUST のホームページを参照願う。)

No Exchange ; このマークは、トランザクション、トラッキング等の匿名性が守られているサイトを示すマークである。

One-to-One Exchange ; このマークは、第 3 者にはトランザクションや個人的なデータは開示されないサイトを示すマークである。

Third Party Exchange ; このマークは、第 3 者にもトランザクションや個人的なデータが開示されるサイトであることを示すマークである。

eTRUST のマークの付与は、今後展開していくガイドラインに沿って「calculator」と呼ばれる者が個別に評価した結果により行われる。また、地域社会が監視する時の判断にも使用できるマークである。さらに、第 3 者の調査と監査を行ない、例えば、事前に認可したサイトか否かの調査、任意のサイトの監視等がある。それらの行為は、保証処理委員会 (K P M G と Coopers&Lybrand) で実施する。

4.8.3.2 質疑応答

(1) マークは、だれが判断して付与するのか。“calculator”では、少しニュアンスが違うのではないか。

“calculator”が判断する。3段階ではなく、3種類と考えてほしい。

(2) マークの偽造の有無の見分けはどのように行なうのか。

見分け方はない。もし、偽ってマークを使用しているサイトがわかれば、処罰されることになる。実際には、eTRUST のサイトに登録された企業リストがあるため、登録された企業が否かはチェックできる。

(3) eTRUST のマークは、認証局についてもすべて適応するものか。

現在の eTRUST のマークは、プライバシーに関するものであり、セキュリティ、認

証局に対応したものではない。

- (4) サイトにアクセスするだけで、個人のアドレスは相手にわかると考えられるが、その個人情報は、eTRUST では、どのように扱うのか。

クッキーのアセス時に、クッキーレベルで対応する方法も考えている。クッキーを受け付けるか否かを各サイトに選択させるような方法も考えている。

- (5) 技術開発企業に対して、指示書等での技術的な対応依頼は考えているか。

企業の中に対しては、eTRUST へ参加をしてもよいという意向をもっている。企業もあるため、eTRUST に参加して注視してもらおうという方法がある。また、eTRUST 自体の強みは、利益を追求する団体でない非営利団体であり、その主旨と存在意義は、各企業が認めてくれていると考えている。

4.8.4 電子商取引との関連

eTRUST は、その設立母体である CommerceNet が中心となり、米国における電子商取引の拡大を目指して設立された民間団体である。CommerceNet の計画見直しの中で、重要な課題として抽出されたプライバシー問題、セキュリティ問題、認証問題について、調査及び検討することが任務であるが、現時点では、プライバシー問題にのみ焦点をあてている。

5 参考資料

5.1 OECDガイドラインの和訳

5.1.1 プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD 理事会勧告 (1980年9月)

理事会は、1960年12月14日のOECD条約第1(c)、3(a)及び5(b)の各項に留意し、加盟国は、国内法及び国内政策の相違にもかかわらず、プライバシーと個人の自由を保護し、かつプライバシーと情報の自由な流通という基本的ではあるが、競合する価値を調和させることに共通の利害を有すること、個人データの自動処理及び国際流通は、国家間の関係に新しい形態を作り上げるとともに、相互に矛盾しない規則と運用の開発を要請すること、個人データの国際流通は経済及び社会の発展に貢献すること、プライバシー保護と個人データの国際流通に係る国内法は、そのような国際流通を妨げる恐れがあることを認識し、加盟国間の情報の自由な流通を促進すること及び加盟国間の経済的社会的関係の発展に対する不当な障害の創設を回避することを決意し、次のとおり勧告する。

1. 加盟国は、本勧告の主要部分である勧告附属文書のガイドラインに掲げているプライバシーと個人の自由の保護に係る原則を、その国内法の中で考慮すること。
2. 加盟国は、プライバシー保護の名目で、個人データの国際流通に対する不当な障害を除去、又はそのような障害の創設を回避することに努めること。
3. 加盟国は、勧告附属文書に掲げられているガイドラインの履行について協力すること。
4. 加盟国は、このガイドラインを適用するために、特別の協議・協力の手続きについてできるだけすみやかに同意すること。

(オーストラリア、カナダ、アイスランド、アイルランド、トルコ、イギリス各国政府は棄権)

5.1.2 プライバシー保護と個人データの国際流通についてのガイドライン

第1部 総論

定義

1. このガイドラインにおいて
 - (a) 「データ管理者」とは、国内法によって、個人データの内容及び利用に関して決定権限を有する者を意味し、そのような、データが、管理者又はその代理人によって、収集、貯蔵、処理、もしくは流布されるかどうかは問わない。
 - (b) 「個人データ」とは、識別された又は識別されうる個人(データ主体)に関するすべての情報を意味する。

(c) 「個人データの国際流通」とは国境を越えて、個人データが移動することを意味する。

ガイドラインの適用範囲

- 2 . このガイドラインは、その処理方法又は、その性質もしくは利用の状況から、プライバシーと個人の自由に対して危険性のある公的又は私的分野の個人データに適用する。
- 3 . このガイドラインは、次のことを妨げるものと解釈されてはならない。
 - (a) 異なる範ちゅうの個人データに対し、その性質及びその収集、貯蔵処理及び流布の状況に応じて、異なる保護措置を適用すること。
 - (b) プライバシーと個人の自由に対して、明らかにいかなる危険性をも含んでいない個人データについて、ガイドラインの適用を除外すること。
 - (c) 個人データの自動処理についてのみガイドラインを適用すること。
- 4 . ガイドラインの第 2 部及び第 3 部に掲げられている諸原則に対する例外は、国家主権、国家安全保障及び公の政策(“ 公秩序 ”)に関係するものをも含め、
 - (a) できるだけ少なくすること。
 - (b) 国民に知らしめること。
- 5 . 連邦国家という特別の場合には、ガイドラインの遵守は、連邦制における権力の分割によって影響を受けることもある。
- 6 . このガイドラインは、最小限の基準とみなされるべきであり、プライバシーと個人の自由の保護のため追加的措置により補充することができる。

第 2 部 国内適用における基本原則

収集制限の原則

7．個人データの収集には、制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らしめ又は同意を得た上で、収集されるべきである。

データ内容の原則

8．個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たれなければならない。

目的明確化の原則

9．個人データの収集目的は、収集時よりも遅くない時点において明確化されなければならない。その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないでかつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである。

利用制限の原則

10．個人データは、第9条により明確化された目的以外の目的のために開示利用その他の使用に供されるべきではないが、次の場合はこの限りではない。

(a) データ主体の同意がある場合、又は、

(b) 法律の規定による場合

安全保護の原則

11．個人データは、その紛失もしくは不当なアクセス・破壊・使用・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない。

公開の原則

12．個人データに係る開発、運用及び政策については、一般的な公開の政策が取られなければならない。

個人データの存在、性質及びその主要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容易に利用できなければならない

個人参加の原則

13．個人は次の権利を有する。

- (a) データ管理者が自己に関するデータを有しているか否かについて、データ管理者又はその他の者から確認を得ること。
- (b) 自己に関するデータを、
 - () 合理的な期間内に、
 - () もし必要なら、過度にならない費用で、
 - () 合理的な方法で、かつ、
 - () 自己にわかりやすい形で、自己に知らしめられること。
- (c) 上記 (a) 及び (b) の要求が拒否された場合には、その理由が与えられること及びそのような拒否に対して異義を申立てることができること。
- (d) 自己に関するデータに対して異義を申立てること、及びその異議が認められた場合には、そのデータを消去、修正、完全化、補正させること。

責任の原則

14 . データ管理者は、上記の諸原則を実施するための措置に従う責任を有する。

第3部 国際的適用における基本原則 --- 自由な流通と合法的制限

15 . 加盟国は、個人データの国内における処理及びその再移出が、他の加盟国に及ぼす影響について配慮すべきである。

16 . 加盟国は単なる通過も含めた個人データの国際流通が阻害されず、安全であることを確保するために、あらゆる合理的かつ適当な手段を講ずべきである。

17 . 加盟国は、自国と他の加盟国との間における個人データの国際流通を制限することを控えるべきであるが、後者が未だガイドラインを実質的に遵守していない場合、又はかかるデータの再移出がその国のプライバシー保護規制を免れようとする場合は、この限りでない。

加盟国は、また、自国のプライバシー法制が、その性格からして特別の規制をしており、かつ他の加盟国が、自国と同等の保護を課していないある種の個人データに関しては、その流通を制限することができる。

18．加盟国は、プライバシーと個人の自由の保護という名目で、これらの保護に必要とする程度を超え、かつ、個人データの国際流通に対して障害を創設することになるような法律や政策及び運用を差し控えるべきである。

第4部 国内実施

19．第2部及び第3部に規定されている諸原則の国内実施に当たって、加盟国は、個人データに関するプライバシーと個人の自由の保護のための法的、行政的又はその他の手続きあるいは制度を確立すべきである。

加盟国は、特に次の事項に努めるものとする。

- (a) 適当な国内法を制定すること
- (b) 行動綱領その他の形式による自主的な規定の制定を奨励し、支持すること。
- (c) 個人に対し、その権利を行使するための合理的な手段を提供すること。
- (d) 第2部及び第3部の諸原則を実施する措置に応じない場合には適当な制裁及び救済手段を提供すること
- (e) データ主体に対する不当な差別がないようにすること

第5部 国際協力

20．加盟国は、ガイドラインの諸原則の遵守状況について、要求があれば他の加盟国に通知すべきである。加盟国は、また、個人データの国際流通及びプライバシーと個人の自由の保護についての手続きが簡明であり、かつガイドラインを遵守している他の加盟国のそれと矛盾しないようにすべきである。

21．加盟国は、次の事項を容易にするための手続きを確立すべきである。

- () ガイドラインに関する情報交換
- () 手続的調査的事項における相互援助

22．加盟国は、個人データの国際流通に関して、適用し得る法を規律する国内的、国際的な諸原則の開発に向けて作業すべきである。

5.2 個人データ処理に係る個人の保護及び当該データの自由な移動に関する 欧州議会及び理事会の指令(EU指令)

5.2.1 EU指令の和訳

第 章 一般条項

第1条 指令の目的

1. 本指令に従って、加盟国は個人データの処理に対する自然人の基本的人権及び自由、特にプライバシー権を保護するものとする。
2. 加盟国は第1項に従って与えられる保護に関係する理由のために、加盟国間の個人データの自由な流通を規制又は禁止してはならないものとする。

第2条 定義

本指令の目的のために、以下のように用語の意味を定義する。

- (a) 「個人データ」とは、特定できる、又は特定できない自然人（データの対象者）に関する全ての情報を意味するものとする。特定できる人物とは、特に身元確認番号の参照によって、又はその人物の肉体的、生理的、精神的、経済的、文化的、経済的アイデンティティによって、直接又は間接に特定することができる者を意味する。
- (b) 「個人データの処理」（処理）とは、自動的な手段であるかどうかに関わらず、個人データに対して行われる作業又は一連の作業を意味するものとする。これには、収集、記録、編成、保存、編集、変更、検索、参照、利用、もしくは移転、公開、その他の方法による開示、もしくは連結、ブロック化、消去又は破壊が含まれる。
- (c) 「個人データのファイリングシステム」（ファイリングシステム）とは集約型であるか分散型であるか、それとも機能又は地理的条件に基づいて分散されているかどうかに関わらず、特定の基準に基づいてアクセスすることのできる個人データの構造を意味する。
- (d) 「管理者」とは、個人データの処理の目的及び手段を決定する自然人、法人、公的機関、政府機関、又はその他の全ての団体を意味するものとする。処理の目的及び手段が国家の又は EC の法律や規則によって決定される場合には、国家又は EC の法律は、管理者又はその指名に対する特定の基準を規定することができる。
- (e) 「処理者」とは、管理者のために個人データの処理を行う自然人、法人、公的機関、政府機関、又はその他の全ての団体を意味するものとする。

- (f) 「第三者」とは、データの対象者、管理者、処理者、及び管理者又は処理者の直接の管理の下で、データを処理する権利を与えられている人物以外の自然人、法人、公的機関、政府機関、又はその他の全ての団体を意味するものとする。
- (g) 「受取人」とは、第三者であるかどうかに関わらず、データの開示の対象となる自然人、法人、公的機関、政府機関、又はその他の全ての団体を意味するものとする。しかし、特別な照会によって、データを受け取る監視機関は受取人とは見なされないものとする。
- (h) 「データの対象者の同意」とは、データの対象者が処理に関する情報を与えられた上で、自分に関する個人データの処理に対する合意を示す特定の自由な意志表示を意味するものとする。

第3条 範囲

- 1 . 本指令は、全部又は部が自動的な手段による個人データの処理、並びに、ファイリングシステムの一部である、又はファイリングシステムの一部とすることを意図している個人データの非自動的な処理に対して適用されるものとする。
- 2 . 本指令は、以下の個人データの処理には適用されないものとする。
 - 欧州統一に関する条約の第5条及び6条に規定されているような、共同体法の範囲外の活動の過程で行われる個人データの処理。また公安、防衛、国家の安全(国家の経済的繁栄を含む)、及び刑法分野での国家活動に関する処理。
 - 自然人によって、純粹に個人的又は家庭的な活動の過程で行われる個人データの処理。

第4条 適用される国内法

- 1 . 各加盟国は、本指令に従って採択した国内規則を以下の場合に個人データの処理に適用するものとする。
 - (a) 管理者が、加盟国の領域内に設立した設備によって処理を行う場合。同じ管理者が複数の加盟国の領域内で設立される場合には、その管理者は、適用される各国内法が定める義務の遵守を確保するために、必要な措置を取らなければならない。
 - (b) 加盟国の領域外ではあるが、国際公法によって国内法が適用される場所に管理者が設立されている場合。
 - (c) 管理者が、EC領域外に位置しているが、加盟国の領域内にある自動又はその他

の設備を個人データの処理のために利用する場合。但し、このような設備がEC領域を通過する目的だけのために利用される場合は、この限りではない。

2. 第1項(c)の状況の下では、その加盟国の領域内で設立された代理店を指名しなければならない。但しこのことは、管理者自身に対して提起される訴訟活動を妨げない。

第 章 個人データの処理の合法性に関する一般規則

第5条

加盟国は本章の規定の制限内で、個人データの処理が適法となる条件をより正確に定めるものとする。

第 部 データの質に関する原則

第6条

1. 加盟国は、個人データが以下の条件を満たすことを確保するものとする。
 - (a) 公正かつ適法に処理されること。
 - (b) 特定、明確、及び合法的な目的のために収集され、このような目的に反した方法で、処理されることのないこと。歴史、統計、又は科学的目的のための、データの処理は、加盟国が適切な保護条項を規定している限り、目的に反しているとは見なされないものとする。
 - (c) 適切、妥当であること。そのデータが収集された目的、及び/又は、それが処理される目的に関して、過度でないこと。
 - (d) 正確であること。必要な場合には、最新の情報を維持すること。データが収集された目的、又はそれが処理される目的に関して不正確又は不完全なデータが消去又は修正されることを確保するために、全ての合理的な手段が取られなければならない。
 - (e) データが収集された目的、又はそれが処理される目的のために必要なだけの期間、データの対象者の特定が可能な形式で保存すること。加盟国は、歴史、統計、又は科学的利用を目的として、個人データを長期間保存するために、適切な保護条項を規定するものとする。
2. 管理者は、第1項の遵守を確保するものとする。

第 部 データ処理の適法性の根拠に関する原則

第7条

加盟国は、個人データが以下の条件を満たす場合にのみ、処理されることを確保するものとする。

- (a) データの対象者が明確に合意を与えた場合。
- (b) データの対象者が当事者である契約の履行のために、処理が必要な場合、又は、契約を締結する前に、データの対象者の要請による段階的作業のために処理が必要な場合。
- (c) 管理者が従うべき法的義務のために、処理が必要な場合。
- (d) データの対象者の重要な利益を保護するために、処理が必要な場合。
- (e) 公衆の利益のために、もしくは管理者又はデータの開示の対象となる第三者に与えられている公的権限の行使による業務のために処理が必要である場合。
- (f) 管理者、データ開示の対象となる第三者、又はその他の当事者の合法的な利益のために、処理が必要である場合。但し、第1条1項に従って保護が要求されるデータ対象者の利益、基本的人権及び自由が上記利益に優先する場合はこの限りではない。

第 部 特別カテゴリーの処理

第8条 特別カテゴリーのデータの処理

- 1 . 加盟国は、人種、民族、政治的見解、宗教、思想、信条、労働組合への加盟に関する情報を漏洩する個人データの処理、もしくは健康又は性生活に関するデータの処理を禁止するものとする。
- 2 . 第1項は、以下のような場合には適用されない。
 - (a) データの対象者が、上記のデータの処理に対して明示の同意を与えた場合。但し、加盟国の法律が、データの対象者の同意によって、第1項の禁止を放棄することができないことを規定している場合はこの限りではない。
 - (b) 処理が労働法の分野で、管理者の義務及び特定の権利を遂行する目的のために必要である場合。但し、適切な保護条項を提供している国内法によって、権限を与えられている場合に限られる。
 - (c) データの対象者が物理的又は法的に同意を与えることができない場合に、データ

の対象者又はその他の者の重要な権利を保護するために処理が必要である場合。

(d) 財団、協会、又はその他の非営利団体によって、政治的、思想的、宗教的、又は労働組合の目的のために、適切な保証を伴う合法的な活動の過程で処理が行われる場合。

但し、その処理は、当該目的に関して団体と定期的に接触している個人又は団体の構成員のみに関係していること、及び、そのデータはデータの対象者の同意なくして第三者に開示されないことを条件とする。

(e) データの対象者によって明示的に公開されたデータ、もしくは司法的請求の提起、行使、又は防御に必要なデータに関する処理。

3 . 第 1 項は、データの処理が予防的医療、診断、看護又は治療の提供、医療サービスの管理に必要な場合、並びに、データが、国内の監視機関によって設定された国内法又は規則に基づいて、職業上の秘密の義務を負う医療専門家によって、又は同様の秘密義務を負うその他の者によって処理される場合には適用されない。

4 . 適切な保養条項の規定に従って、加盟国は重要な公衆の利益を理由として、第 2 項に規定されているものに加え、国内法又は監視機関の決定により例外を規定することができる。

5 . 犯罪、刑法上の起訴、又は防衛問題に関するデータの処理は、公的機関の管理の下でのみ行うことができる。但し、国内法に基づいて、適切な特定の保養条項が規定されている場合には、国内規則に基づいて、加盟国はこの規定を軽減することができる。しかし、刑法上との起訴に関する完全な登録は、公的機関の管理のもとでのみ維持することができる。

加盟国は、行政的制裁又は民事訴訟に関するデータも公的機関の管理の下で処理されるべきことを規定することができる。

6 . 第 4 項及び 5 項に規定されている、第 1 項の軽減は、委員会に対して通知されるものとする。

加盟国は、国内識別番号又はその他の一般的に適用される識別データを処理することができる条件を定めるものとする。

第 9 条 個人データの処理と表現の自由

加盟国は、プライバシー権と表現の自由に関する規則とを調和させる必要があると認めら

れるジャーナリズム、芸術、文学のためにのみ行われる個人データの処理に対して、本章、第4章及び第6章からの規定の免除又は軽減を定めるものとする。

第 部 データの対象者に与えられる情報

第10条 データの対象者からデータを収集する場合の情報

加盟国は、データが収集されるデータの対象者に対して、管理者又はその代理人が、少なくとも以下の情報を提供しなければならないことを定めるものとする。但し、すでにデータの対象者が知っている場合はこの限りではない。

- (a) 管理者及びその代理人がいる場合はその者の氏名。
- (b) データが処理される目的。
- (c) 次に示すような追加情報。
 - データの受取人又は受取人の分類。
 - 質問に対する回答が義務であるのか、任意であるのかに関する情報、及び回答しなかつた場合に考えられる結果。
 - 対象者に関するデータにアクセスし、修正を行う権利の有無。
必要がある限り、データが収集される特別な状況を考慮にいれて、データの対象者に対して、公正な処理を保証すること。

第11条 データが、データの対象者から収集されなかった場合の情報

1. データがデータの対象者から取得されなかった場合には、加盟国は管理者又はその代理人が個人データの記録時、又は第三者に対して開示する予定がある場合には、最初にデータが開示される時より早い時点で、データの対象者に対して少なくとも以下の情報を提供しなければならないことを規定するものとする。但し、データの対象者がすでに知っている場合はこの限りではない。

- (a) 管理者及びその代理人がいる場合はその者の指名。
- (b) データが処理される目的。
- (c) 次に示すような追加情報。
 - 関係データの分類。
 - 受取人又は受取人の分類。
 - データの対象者に関するデータにアクセスし、修正を行う権利の有無。

必要がある限り、データが収集される特別な状況を考慮にいれて、データの対象者に対して、公正な処理を保証すること。

2. 特に統計、歴史、科学調査のための処理に対して、情報の提供が不可能、又は過度の困難を伴う場合、もしくは記録又は開示が法律によって明示的に規定されている場合は、第1項は適用されないものとする。このような場合に加盟国は、適切な保護条項を規定するものとする。

第 部 データの対象者のデータに対するアクセス権

第12条 アクセス権

加盟国は全てのデータの対象者に対して、管理者から以下のことを取得する権利を保証するものとする。

1. 制限なしに、合理的な間隔において、過度の遅れ及び費用を伴うことなく、以下の情報を取得すること。
 - データの対象者に関するデータが処理されているのかどうかに関する確認、及び少なくとも処理の目的、関係データの分類、データが開示される受取人又は受取人の分類に関する情報。
 - 処理されているデータの判読可能な形式での通知、及びデータの収集源に関する入手可能な情報。
 - 少なくとも第15条1に規定されている自動判断の場合には、データの対象者に関するデータの自動的処理に関わる論理の知識。
2. 然るべき場合には、特にデータの不完全又は不正確な性質を理由とする、処理が本指令の規定に従っていないデータの修正、消去又はブロック化。
3. 第2項に従って行われた修正、消去又はブロック化のデータが開示された第三者に対する通知。但し、これが不可能又は過度の困難を伴うことが確認された場合はこの限りではない。

第 部 免除と制限

第13条 免除と制限

1. 加盟国は、制限が権利を保護するために適切である場合には、第6条1、10条、11条1、12条及び21条に規定されている義務及び権利の範囲を、以下の事柄を保

護するために制限する法的措置を採択することができる。

- (a) 国家の安全。
- (b) 防衛。
- (c) 公安。
- (d) 刑事的犯罪又は規制されている職業に対する倫理違反の防止、捜査、発見及び起訴。
- (e) 金融、財政及び税金に関する事柄を含む加盟国及び欧州連合の重要な経済的又は財政的利益。
- (f) (c) (d) 及び (e) 項で触れた場合に関して、公的機関の業務に絶続的又は非継続的に関わる監視、捜査又は規制職務。
- (g) データの対象者又はその他の者の権利及び自由の保護。

2 . 特に、特定のデータの対象者に関する、措置又は決定を目的としない場合は、適切な法的保証に従って、加盟国は法的措置によって第 1 2 条に規定されている権利を制限することができる。これには、データが歴史的調査の目的だけのために処理される場合、又は統計を作成する目的だけのために必要な期間の間、個人的な形式で保存される場合などが含まれる。

第 部 データの対象者の拒否権

第 1 4 条 データの対象者の拒否権

加盟国はデータの対象者に以下の権利を付与する。

- (a) 少なくとも第 7 条 (c) 及び (f) 条に規定されている場合には、常に対象者に関するデータの処理に対する特別な状況に関して、強制的かつ合法的に、拒絶する権利。但し、国内の法律に、反対の主旨の規定がある場合には、この限りではない。正当な拒絶があった場合には、管理者によって始められた処理に、もはやその個人のデータを含むことができない。
- (b) 要請によって、管理者が直接的商業目的のために処理する予定のある、対象者に関する個人的データの処理を、費用を払うことなく拒絶する権利。
個人データが最初の第三者に開示される前に、また第三者の直接的商業目的のために利用される前に、通知を受ける権利、及び費用を払うことなく、このような開示及び利用を拒絶する権利が明示的に与えられる。

加盟国は、データの対象者が第（b）項の第1文に規定されている権利の存在を知っていることを確保するために必要な措置を取るものとする。

第15条 個人に関する自動的判断

1. 加盟国は、対象者の業務成績、信用度、行為などの対象者に関する個人的な事柄を評価することを意図した、データの自動的な処理のみに基づく、対象者に関して法的な効果を有し、又は対象者に重大な影響を与える決定の対象とならない権利を全ての者に与えるものとする。
2. 以下の条件を満たす場合には、加盟国は本指令の他の条文に従って、第1項で触れた判断を行うことができることを規定するものとする。
 - (a) 契約の締結又は履行の過程で行われる決断。但し、データの対象者からの要求が満たされ、またデータの対象者に自らの見解を防衛することを認める措置のような、対象者の法的権利を守るための適切な措置が存在することを条件とする。
 - (b) 法により認められている判断。但し、その法は、データの対象者の正当な権利を保護するための措置を規定している必要がある。

第 部 処理の秘密保持及び安全

第16条 処理の秘密保持

個人データにアクセスすることができる管理者又は処理者の監督の下で働いているものは、処理者自身を含め、管理者からの指示に基づく場合を除き、個人データを処理してはならない。但し、法により処理が要請される場合は、この限りではない。

第17条 処理の安全

1. 加盟国は、特に、処理がネットワーク上でのデータの伝送を伴う場合、及びその他の全ての不法な処理形式に対して、管理者が個人データを不慮の又は不法の破壊、不慮の損失及び無許可の変更、開示又はアクセスから保護するために、適切な技術的及び組織的措置を取らなければならないことを規定するものとする。

最新技術及び、その実施の費用を考慮に入れて、かかる措置は、処理によって生じうる危険、及び処理されるデータの性質に対して適切な安全のレベルを確保するものとする。

2. 加盟国は、管理者が処理を自らのために行う場合には、実施される処理に関する、技術的安全措置及び組織的措置に対して、十分な保証を提供する処理者を選ぶべきこと、及びこのような措置の遵守を確保しなければならないことを規定するものとする。
3. 処理者による処理の実行は、処理者を管理者に対して拘束し、特に、以下の事柄を規定する契約又は法律行為に準拠しなければならない。
 - 処理者は、管理者の指示のみに基づいて行動すべきこと。
 - 処理者の所在する加盟国の法律によって定義され、第1項に規定されている義務は処理者にも課せられるべきこと。
4. 証拠を維持するために、データの保護に関する契約又は法律行為、及び第1項で触れた措置に関する条件の一部は、書面又はその他の同等の形式によるものとする。

第 部 通知

第18条 監視機関に通知する義務

1. 加盟国は、管理者又はその代理人が、1つの目的又は複数の関係する目的を意図した全体的又は部分的に自動的な一連の処理作業を実行する前に、第28条で触れる監視機関に通知しなければならないことを規定するものとする。
2. 加盟国は、以下の場合のみに、以下の条件に基づいて、通知義務の簡略化又は免除を規定することができる。
 - 処理されるデータを考慮に入れて、データの対象者の権利及び自由を害するおそれの少ないと見なされる処理作業の分類に対して、管理者又はその代理人が、処理の目的、処理されるデータ、データの分類、データの対象者の分類、データが開示される受取人又はその分類、データが保存される期間を指定した場合。
 - 管理者が、適用される国内法に従って、特に以下の事柄に責任を有するデータ保護職員を指名した場合。
 - 他から独立して、本指令に基づいて制定される国内規則の適用を確保すること。
 - 第21条2に掲げられている情報項目を含むデータに関し、管理者が行った処理作業の記録を維持すること。これによって、処理作業がデータの対象者の権利及び義務を害しないことを確保すること。
3. 加盟国は、登録の維持を唯一の目的とする処理作業が、法律又は規則に従って、国民

に情報を提供し、国民又は正当な権利を有する全ての者による参照のために開放することを意図している場合には、第1項は適用されないことを規定することができる。

4. 加盟国は、第8条2(d)で触れた場合又は処理作業に関して、通知義務の免除又は簡略化を規定することができる。
5. 加盟国は、個人データに関するある種の又は全ての自動的でない処理作業に対して、通知義務を課することができる。またこのような作業に対して、通知義務の簡略化を規定することもできる。

第19条 通知の内容

1. 加盟国は、通知に含まれるべき情報を指定するものとする。これには少なくとも以下のものが含まれる。
 - (a) 管理者及びその代理人がいる場合には、その者の氏名及び住所。
 - (b) 目的及び処理の目的。
 - (c) データの対象者の分類、及びデータの対象者に関連するデータ又はデータの分類の記述。
 - (d) データが開示される予定の受取人又は受取人の分類。
 - (e) 第三国に対するデータの移動の予定。
 - (f) 処理の安全を確保するために、第17条に従って取られた措置の適切性に関する予備査定のための一般的説明。
2. 加盟国は、第1項で触れた情報に影響を与える変更を、監視機関に通知しなければならないデータ処理を指定するものとする。

第20条 事前の検査

1. 加盟国は、データの対象者の権利及び自由に特有の危険をもたらすおそれのある処理作業を指定し、かかる処理作業が始められる前に検査が行われることを確保するものとする。
2. かかる事前の検査は、管理者からの通知を受けた後に、管理者又はデータ保護職員によって行われる。データ保護職員は、疑問点があれば監視機関に相談しなければならない。
3. 加盟国は、国会によって決議された措置の準備段階で、又はかかる決議に基づいて、

データ処理作業の性質を定義し、適切な保護集項を規定するために、上記検査を行うことができる。

第21条 処理作業の公開

1. 加盟国は、処理作業が公開されることを確保するための措置を取るものとする。
2. 加盟国は、第18条に従って通知された処理作業の登録が、監視機関によって維持されるべきことを規定するものとする。

登録には、少なくとも第19条1の(a)から(e)に掲げられている情報が含まれるものとする。

誰でも、この登録を検査することができるものとする。

3. 加盟国は、通知義務の対象とならない処理作業に関して、加盟国に指定された管理者又はその他の団体が、少なくとも第19条1の(a)から(e)に掲げられている情報を、あらゆるものに、適切な形式で提供することを規定するものとする。

加盟国は、登録の維持を唯一の目的とする処理作業が、法律又は規則に従って、国民に情報を提供し、国民又は正当な権利を有する全ての者による参照のために開放することを意図している場合には、本条項は適用されないことを規定することができる。

第 章 司法的救済、責任及び罰則

第22条 救 済

司法当局への照会の前に、とりわけ第28条で触れる監視機関によって規定される行政的救済を害することなく、加盟国は、データ処理に適用される国内法が保証する権利の全ての侵害に対して、司法的救済を受ける権利をあらゆる者に与えるものとする。

第23条 責 任

1. 加盟国は、遵法な処理作業、又は本指令に従って採択された国内規則に反する行為によって損害を被った全ての者に、管理者から損害賠償を受け取る権限を与えるものとする。
2. 管理者は、損害の原因となった事態に対して責任を有しないことを証明すれば、この責任の全部又は一部から免除されることができる。

第24条 制裁

加盟国は、本指令の条文の完全な実施を確保するために、適切な措置を採択するものとし、特に本指令に従って採択された国内規定の違反に対して課される制裁に関して規定するものとする。

第 章 第三国に対する個人データの移動

第25条 原則

1. 加盟国は、処理されている、又は後に処理される予定の個人データの第三国への移動は、当該第三国が適切なレベルの保護を提供している場合に限られることを規定するものとする。但し、本指令に従って採択された国内規定に対する遵守を害しないことを条件とする。
2. 第三国によって提供される保護レベルの適切性は、一連のデータの移転作業を取り巻く全ての環境に照らして査定されるものとする。特にデータの性質、提案された処理作業の目的及び期間、データの移転元の国及び最終目的国、当該第三国で効力を有する一般的な及び分野別の法律、当該第三国で遵守されている職業上の規則、及び防衛上の措置が考慮に入れられるものとする。
3. 加盟国及び委員会は、第三国が第2項の意味の枠内で適切な保護のレベルを確保していないと考える場合には、互いに情報を交換するものとする。
4. 委員会は、第31条2に規定されている手続きに基づいて、第三国が本条の第2項の意味の枠内で、適切なレベルの保護を確保していないことを認定した場合には、加盟国は当該第三国に同種のデータの移転を妨げるために必要な措置を取るものとする。
5. 委員会は適切な時に、第4項に従って行われた認定から生じた状況を修正するために交渉を行うものとする。
6. 委員会は第31条2に規定されている手続きに従って、個人のプライバシー権、基本的自由及び権利の保護に対する第三国の国内法、又は委員会が特に第5項で触れた交渉の結果に基づいて実施した国際的介入によって、本条第2項の枠内で適切なレベルの保護を確保していることを認定することができる。

加盟国は、委員会の決定に従うために必要な措置を取るものとする。

第26条 免除

1. 特別な事情に関する国内法に反対の主旨の規定がない限り、第25条からの免除とし

て、加盟国は、第25条2の意味の枠内で、適切な保護レベルを確保していない第三国に対する個人データの一連の移転は、以下の条件に基づいて行うことができることを規定するものとする。

- (a) データの対象者が提案された移転に対して、明確な同意を与えること。
- (b) その移転がデータの対象者と管理者との間の契約の履行、又はデータの対象者の要請による契約前の措置の実施のために必要であること。
- (c) 移転がデータの対象者のために管理者と第三国との間で締結された契約の作成又は履行のために必要であること。
- (d) 移転が重要な公衆の利益に基づくこと。もしくは、法的請求の提起、行使又は防御のために必要であること。
- (e) 移転がデータの対象者の重要な権利を保護するために必要であること。
- (f) 法律又は規則に従って、国民に情報を提供し、国民又は正当な権利を有する全ての者による参照のために開放することを意図している登録から移転が行われること。但し、個々の場合において、参照に関する法律に規定されている条件が満たされていることを条件とする。

2 . 管理者が、個人のプライバシー権、基本的人権及び自由の保護に関する保証、及び対応する権利の行使に関する十分な保証を提示する場合には、加盟国は第1項の規定を害することなく、第25条2の意味の枠内で適切な保護レベルを確保していない第三国に対する個人データの一連の移転を許可することができる。このような保証は、特に、適切な契約の条文によって設定することができる。

3 . 加盟国は、第2項に従って与えた許可に関して、委員会及びその他の加盟国に通知するものとする。

いずれかの加盟国又は委員会が個人のプライバシー権、基本的人権及び自由の保護に関する理由に基づいて反対する場合には、委員会は第31条2に規定されている手続きに従って、適切な措置を取るものとする。

加盟国は、委員会の決定に従うために必要な措置を取るものとする。

4 . 委員会が第31条2に規定されている手続きに従ってある標準的な契約の条文が、第2項によって要求される十分な保証を提供していると決定した場合には、加盟国は委員会の決定に従うために、適切な処置を取るものとする。

第 章 行動規約

第 27 条

1. 加盟国及び委員会は、加盟国が本指令に従って採択する国内規則の適切な実施に役立てるために、様々な分野に特有な特徴を考慮にいれて、行動規約の作成を推進するものとする。
2. 加盟国は、監視機関に提出するために、国内規約案を作成し、又は現存する国内規則を修正又は拡張する意思のある貿易協会及びその他の分類の管理者を代表する団体に対して、規則を制定するものとする。
加盟国は、とりわけ、提出された規約案が本指令に基づいて採択された国内規則に従っているかどうかを確認することに関して、監視機関に対して規則を制定するものとする。規約案が適切であるように思われる場合には、監視機関はデータの対象者又はその代理人の意見を求めるものとする。
3. 作成委員会の規約及び現存する委員会の規約に対する修正又は拡張は、第 29 条に規定されている作業部会に提出することができる。この作業部会はとりわけ、提出された規則案が本指令に従って採択された国内規則に従っているかどうかを決定するものとする。規約案が適切に思われる場合には、作業部会はデータの対象者又はその代理人の意見を求めるものとする。委員会は、作業部会によって承認された規約に対して、適切な公開を確保することができる。

第 章 個人データの処理に対しての個人の保護に関する監視機関及び作業部会

第 28 条 監視機関

1. 各加盟国は、1 つ以上の公共機関が、本指令に従って加盟国が採択した規則の国家領域内での適用を監視することに責任を有することを規定するものとする。
このような機関は委任された職務を、完全に独立して遂行するものとする。
2. 加盟国は、個人データの処理に対する個人の権利及び自由の保護に関する行政的措置又は規制を作成する場合には、監視機関に相談すべきことを規定するものとする。
3. 各監視機関は以下の権限を与えられる。
 - 処理作業の目的物となるデータにアクセスする権限、監視職務の遂行のために必要な全ての情報を収集する権限のような調査権。
 - 例えば、処理作業が実施される前に、第 20 条に従って勧告を行う権限、そのような

勧告の適切な公開を確保する権限、データのブロック化、消去又は破壊を命じる権限、処理に対する一時的又は確定的な禁止を命じる権限、管理者に警告又は懲戒を与える権限、問題点を国会又はその他の政治機関に照会する権限などの効果的な介入権。

- 本指令に従って採択された国内規則の違反があった場合に、訴訟を起こし、又はこのような違反を司法当局に通知する権限。

不満の対象となった監視機関の決定は、法廷を通じて訴えることができる。

4. 各監視機関は、個人データの処理に対する個人の権利及び自由に関して、個人又は個人を代表する協会からの請求を受けるものとする。関係個人は、請求の結果に関して通知を受けるものとする。

各監視機関は、本指令の第 13 条に従って採択された国内規則が適用される場合には、個人によるデータの処理の合法性に関する調査に対しての請求を受けるものとする。

個人は、少なくとも調査が行われたことの通知を受けるものとする。

5. 各監視機関は定期的にその活動に関して、報告書を作成するものとする。その報告書は公開されるものとする

6. 各監視機関は、当該処理に対してどの国内法が適用されるかに関わらず、自らの加盟国の領域内において、第 3 項に従って与えられた権限を行使することができる。各監視機関はその他の加盟国の監視機関によって、その権限の行使を求められることがある。

監視機関は、特に全ての有用な情報を交換することによって、職務の遂行に必要な範囲で、お互いに協力するものとする。

7. 加盟国は、監視機関の構成員及び職員が、雇用が終了した後でも、アクセスした秘密情報に関して職業上の秘密義務を負うことを規定するものとする。

第 29 条 個人データの処理に対する個人の保護に関する作業部会

1. 個人データの処理に対する個人の保護に関する作業部会がここに設立される。(以下作業部会という)

作業部会は、助言を与える権限及び独立して行動する権限を有するものとする。

2. 作業部会は監視機関の代表者又は各加盟国によって指定された 1 つ以上の監視機関の代表者、E C の機関及び団体のために設立された 1 つ以上の監視機関の代表者、及び委員会の代表者から構成される。

作業部会の各構成員は、その者が代表する協会又は1つ以上の監視機関から指名されるものとする。加盟国が1つ以上の監視機関を指定している場合には、加盟国は、共同代表を指名するものとする。同様のことがE Cの機関及び団体に対して設立された監視機関に対しても当てはまるものとする。

3. 作業部会は、監視機関の代表者の単純多数決によって決定を行うものとする。
4. 作業部会は議長を選任するものとする。議長の任期は2年とする。但し、この任期は更新しうるものとする。
5. 作業部会の事務局は、委員会が提供するものとする。
6. 作業部会は、独自の手続規則を採択するものとする。
7. 作業部会は、議長の独自の判断によって、もしくは監視機関の代表者の要請、又は委員会の要請によって議題に挙げられた事柄を検討するものとする。

第30条

1. 作業部会は、以下の事柄を行うものとする。
 - (a) 本指令に基づいて採択された国内措置の統一的な適用に貢献するために、問題点を検討すること。
 - (b) E C内及び第三国内での保護レベルに関して、委員会に意見を述べること。
 - (c) 本指令に対する修正案、個人データの処理に対しての自然人の権利及び自由を保護するための追加又は特定の措置、及びかかる権利及び自由に影響を与える、提案されたその他のE Cの措置に関して、委員会に助言を与えること。
 - (d) E Cレベルで作成された行動規約に関して、意見を述べること。
2. 作業部会が、E C内での個人データの処理に対しての個人の保護の同等性に影響を与えるおそれのある相違が、加盟国間の法律又は慣習の間で生じていることを確認した場合には、それを委員会に通知するものとする。
3. 作業部会は、独自の判断でE C内の個人データの処理に対する個人の保護に関する全ての問題点に関し、勧告を行うことができる。
4. 作業部会の意見及び勧告は、委員会及び第31条で触れる専門委員会に通知されるものとする。
5. 委員会は作業部会に対して、その意見及び勧告に対応して行った行動を通知するものとする。この通知は報告書によって行い、この報告書は欧州議会及び評議会に対して

も提出されるものとする。この報告書は公開されるものとする。

6. 作業部会は、EC内及び第三国内での個人データの処理に対しての自然人の保護に関する状況に関して、年次報告書を作成し、それを委員会、欧州議会、欧州評議会に提出するものとする。この報告書は、公開されるものとする。

第 章 EC が実施する措置

第 3 1 条 専門委員会

1. 委員会は加盟国の代表者によって構成され、委員会の代表者が議長を務める専門委員会の支援を受けるものとする。
2. 委員会の代表者は専門委員会に、措置の草案を提出するものとする。専門委員会はその事柄の緊急性に従って、議長が定めた期限内に、その草案に関する意見を提出するものとする。

その意見は、条約の第 1 4 8 条 (2) に規定されている多数決によって決議されるものとする。専門委員会内の加盟国の代表者の議決は、当該条文に規定されている方法によって数えられるものとする。議長は、議決権を有しないものとする。

委員会は、計画された措置が、専門委員会の意見に従っている場合には、それを採択するものとする。

計画された措置が、専門委員会の意見に反しているか、又は専門委員会の意見が提出されなかった場合には、委員会は直ちに、当該措置に関する提案を評議会に提出するものとする。評議会は、定足数によって行動するものとする。

3 ヶ月の諮問期間の内に、評議会が行動を起こさなかった場合には、提案された措置は、委員会によって採択されるものとする。

最終条項

第 3 2 条

1. 加盟国は、本指令の採択から少なくとも 3 年以内に本指令を遵守するために必要な法律、規則及び行政規定を発効させるものとする。

加盟国は、このような規定を採択する際には、本指令に対する参照を加え、公報を出版する場合には、参照文を添付するものとする。このような参照を作成する方法については、加盟国が規定するものとする。

2. 加盟国は、本指令に基づいて採択された国内規定が発効した日にすでに実施されている処理が、その日から3年以内にかかる規定を遵守することを確保するものとする。
上記の副項の軽減として、加盟国は本指令の実施のために採択された発効日にすでに行われている、手作業のファイリングシステムによるデータの処理を、本指令が採択された日から12年以内に第6、7及び8条に従わせるものとする。但し、加盟国は、データの対象者に対して、特にアクセス権を行使する時に、要請によって、不完全、不正確、又は管理者が追求する合法的な目的に反した方法で保存されているデータの修正、消去又はブロック化を行う権利を与えるものとする。
3. 第2項の軽減として、加盟国は適切な保護条項に従って、歴史調査の目的だけのために維持されているデータは、本指令の6、7及び8条に従う必要がないことを規定することができる。
4. 加盟国は、本指令の対象となる分野において採択した国内法の規定を委員会に対して通知するものとする。

第33条

委員会は第32条1に記載されている日付から3年以内の時点以降、定期的に欧州評議会及び欧州議会に対して、本指令の実施に関し、報告書、及び必要があれば適切な修正案を添付して、報告を行うものとする。この報告は公開されるものとする。

委員会は、特に自然人に関する音響及び画像データの処理に対しての、本指令の適用を調査し、情報技術の発展、及び情報化社会の発展状況を考慮に入れて、必要と見なされる適切な提案を提出するものとする。

第34条

本指令は、各加盟国を対象とし、以下の者によって署名された。

欧州議会議長

欧州評議会の論拠声明

. 序

1990年6月18日、委員会は、個人データの処理に対しての個人の保護に関する指令の提案を提出した。この提案は、条約の第100条a及び113条に基づいて作成された。

欧州議会は1992年3月11日に最初のリーディングに基づく見解を発表し、委員会の提案に対する多くの修正を提案した。

経済社会委員会は1991年4月24日に、その見解を発表した。

このような見解を考慮に入れて、委員会は1992年10月15日に、指令に対する修正提案を提出した。

1995年2月20日、欧州評議会は、条約の189条b(2)に従って、共通方針を採択した。

・目的

指令に対する提案は、情報化社会が欧州の市民に受け入れられる方法で発展するために不可欠な、明確かつ安定した法的枠組みの一部を形成する。

もっと具体的には、その提案は個人データがEC内で自由に移動できることを確保し、個人データの処理に関して、全ての加盟国で、個人の保護に関する同等のレベルの保護を設定することにより、生じるおそれのある競争の歪み及び企業の移転の危険を防止するために作成された。

高いレベルの保護は、一方では、自らの責任の下で処理作業に携わっている個人、公共機関、企業又は協会に対して義務を課することによって、他方では、データの処理の対象となる自然人の権利を定めることによって達成することができる。

管理者の義務は、とりわけ、データの質、及び特定かつ合法的な目的のための使用に関連する。合法性とは、データの対象者の同意、無許可のアクセスを防止するための技術的安全性、及び国内監視機関に対する処理の通知を含む、処理に対する基礎的事項に関連する。

自然人の権利は、様々な状況の下で、その者に関係するデータが処理される時に通知を受ける権利、何のデータであるかを調べる権利、データが不正確である場合には、それを修正する権利、処理を拒絶する権利などが含まれる。

・共通方針の分析

A．包括的見解

共通方針は、最初のリーディングに基づいて欧州議会が表明した憂慮を非常に重視している。

特に共通方針は、公共部門及び民間部門に関する規則の間の正式の区別を廃止することに関して、欧州議会が提案した主な修正を検討した。これは、本文の完全な再構成を必要とした（修正7から29、39から41、118から119）。

共通方針はまた、データの様々な使用に関する保護の実施に対して、広義のコンセプトを採択することに関する欧州議会のアイデアを採用することを検討した。この目的のために、「処理」のコンセプトが採用された。「ファイリングシステム」というコンセプトは、今後は手作業によるデータ処理に関してのみ使用されるようになるであろう。欧州議会は、「ファイリングシステム」というコンセプトは時代遅れであり、コンピュータ化及びテレコミュニケーションの発展の文脈にはそぐわないことを示唆した。

また本文の明確化又は簡略化、もしくは加盟国間での同等の保護を保証し、しかも保護レベルの低下につながらない柔軟な措置を導入するために多くの修正がおこなわれた。これによって、効果的で、煩雑でない方法によって、一般的原則を様々な個人データの処理方法に適用することが可能になった。

さらに、欧州評議会及び委員会は、第100 a条が指令のための適切な法的基礎であることを認識し、それゆえ、委員会が修正提案の中で、法的基礎として提出した113条を排除した。

欧州評議会は、第三国に対する個人データの移転に関する指令の第25条及び26条は、それ自体が通商政策の目的を追求しているわけではないことを認識した。これらの条文は、第三国に対するデータの移転に関して、水も漏らさないシステムをつくるために、当該条文と一体をなすその他の指令の条項から、当然の結果として生じたものである。

B．個々の条文に対する見解

1．共通見解の中で考慮に入れられた欧州議会の修正案

(a) 定義（第2条）

データの収集段階及び様々な形式のデータの移転が処理の定義に含まれた（修正10、15、16及び34）。

個人データがより詳細に定義された(修正12)。

第三国及び処理の定義が加えられた（修正18、134）。

(b) データの質に関する原則 (第 6 条)

処理の目的によるデータの最大保管期間に対する例外が、歴史、統計又は科学的目的のために保管されるデータに対して導入された(修正 6 0)。

データが収集される目的は、収集の前に通知されなければならないとされた (修正 5 9)。

(c) 特別なカテゴリーの処理 (第 8 条)

非営利団体による、政治的、思想的、宗教的、又は労働組合の目的のための個人データの処理は、それが構成員に関する機密性の高いデータに関連する場合には、特別の免除が与えられること。但し、その他の場合には、禁じられるべきこと (修正 1 4 9)。

犯罪及び刑法上の起訴などに関連するデータの処理の柔軟性を求める欧州議会の希望は、本文に具体化された (修正 6 5)。

(d) データの対象者の権利 (第 1 0、 1 1 及び 2 2 条)

データの対象者の権利は、特に以下の点で強化及び簡略化された。

- 通知を受ける権利は、データの収集源及び、ある種の処理作業に関する論理にまで拡張された (修正 4 6 及び 4 8)。
- アクセス権は第三者からの制約なしに行使できなければならないこと (修正 1 3 2)。
- 特に商業目的の処理に関して、拒否権はいつでも行使することができること (修正 3 0 及び 1 4 5)。
- 加盟国によって提供される上訴の機会が、指令によって与えられる全ての権利に拡張された。この点に関して、公共部門に対して責任を有する個人に対しても制裁を適用すべきであるとする欧州議会の要請が前文 5 5 に加えられたことを指摘しなければならない (修正 5 2 及び 7 7)。

(e) 処理の通知及び監視機関による事前の検査 (第 1 8、 1 9 及び 2 0 条)

複雑な手続きを減らし、効率化を進めるために、通知手続きに制限が加えられた。加盟国は処理がデータの対象者の権利及び自由を損なわない場合、もしくは政治的、思想的、宗教的団体又は労働組合によって行われる場合には、通知義務からの免除又は通知の簡略化を規定することができる。實際上、非常に多くの処理作業が、このような免除又は簡略化の対象となることができる (特に欧州議会の修正 2 3 で言

及されている処理)。

加えて、個人の権利及び自由に特有の危険をもたらす処理作業は、前もって監視機関の検査を受けるべきであるとする原則が検討された。欧州議会によって提示された、かかる処理作業の例は前文に参考として掲げられた(修正40、42、118及び119)。

このことによって、加盟国は、実務の多様性、及びデータ処理の発展に関する相違を必然的に生じる各国家の特徴に、手続きを適合させることが可能になる。

監視機関が通知を受け、維持している処理作業の登録の国民による調査が採択された(修正37及び39)。

(f) 行動規約(第27条)

国家及び欧州レベルでの行動規約の作成は、様々な分野の特徴にあわせた方法で、指令の原則を実施するために推奨される。加えて監視機関、第29条で触れている個人の保護に関する作業部会、データの対象者及びその代理人は、このような規約の作成に関わることができる(修正72及び91)。

(g) 監視機関(第28条)

各加盟国は、加盟国の連邦の構成を考慮に入れて、指令に従って採択された規定の適用を監視する1つ以上の監視機関を設立しなければならない(修正84)。監視機関の権限には、データのブロック化、消去又は破壊を命じること、もしくは処理を禁じることが含まれる(修正86)。監視機関は、定期的に報告書を公開しなければならない(修正87)。

(h) 個人の保護に関する作業部会(第29条)

欧州議会によって提案された以下の業務が検討された。

- 指令に基づいて採択された国内措置の適用に関する見解の表明。
- E C内及び第三国内での保護レベル、及び個人の権利と自由を保護するための措置に対する見解の表明。
- 独自の措置に関する見解の表明。

委員会は、作業部会の意見に基づいて行った措置を作業部会に通知するために、報告書を作成、公開し、欧州議会及び欧州評議会にも提出するものとする(修正90、91及び92)。

(i) 最終条項(第36条)

委員会が定期的に欧州議会及び欧州評議会に提出する報告書は公開されなければならない(修正95)。

2. 欧州評議会の共通方針による提案に対するその他の修正

(a) 定義(第2条)

データの対象者に関して処理の透明性を確保するために有用な受取人の定義が加えられた。

(b) 手作業のファイリングシステムによるデータ(第2条及び33条)

これまで手作業によるファイリングシステムを採用していなかった加盟国での、指令の実施を容易にし、指令の一部の条項の適用を促進するために、12年間の移行期間が設けられた。

(c) 適用される国内法(第4条)

欧州評議会は、管理者の設立の場所に関して、委員会が提案した統合市場に対する一般的な基準を採用した。又、欧州評議会は、管理者の設立のコンセプト(前文19)、処理者の安全義務(第17条)、領域内で行われる処理作業に対しての監視機関の権限(第28条)に対して、有用な説明を与えた。

(d) 機密性の高いデータの処理(第8条)

特に、医療又は雇用分野における重要な必要性に対応するために、適切な保護条項に従って、人種、民族、信条、健康、性生活に関するデータに対する禁止の例外が加えられた。

重要な公衆の利益のために規定された免除、及び刑法に関するデータの処理に対する規則からの免除は、委員会に対して通知しなければならない。

(e) 表現の自由(第9条)

欧州評議会は、ジャーナリズムの目的のためのデータの処理を指令の範囲に加えようとする委員会の方針を承認した。このような処理及び芸術又は文学的表現の目的のために行われる処理に対しては、プライバシー権と、この分野で必要な表現の自由とを調和させるために、特別な調整が必要となるであろう。この調整は、加盟国によって実施される。

(f) 統計、歴史、又は科学的目的のための処理

指令の「枠組み」的性格を維持する一方で、欧州評議会は、統計、歴史及び料学的利用のためのデータ処理に対して、最大のデータ保管期間に対する免除に関して、

有用な説明を加えた（第6条1（e））。特に第6条1（b）では、このような目的のための処理作業と、その他の目的のために収集されたデータとの互換性に関して、第11条では、個人に対する情報の提供に関して規定している。又、このような目的のために処理されるデータに対するアクセス権からの選択的免除の範囲が拡張された（第13条2）。

（g）処理の透明性（第10、11及び21条）

データの対象者に対して、関連するデータの処理に関する情報を提供する義務は、処理が実行される環境の多様性に対応するために、より柔軟なものとなった（第10条及び11条）。さらに、修正前の第10条に規定されていた、自らのデータが処理されていることを知る権利を全てのものに確保する加盟国の義務は、第21条に処理作業の公開を確保する義務として組み込まれた。

（h）免除及び制限（第13条、修正前の14条）

情報の提供及び処理の透明性に関する条項（修正前の第11、12条及び21条、修正後の第10、11及び21条）に規定されている免除及び制限は、アクセス権に対する免除を規定していた修正前の14条に挿入された。

この条文に掲げられている権利を保護するために、免除及び制限の範囲は、第6条に規定されている処理の目的の原則に対して拡張された。

免除及び制限は、立法的措置によって採択されなければならないことが規定された。アクセス権が規制される場合に、データの対象者の要請によって行われる監視機関による調査の保証措置が、第28条に組み込まれた。

（i）処理の安全（第16条及び17条）

秘密保持に関する条項は、独立の条項（第16条）として規定された。管理者と処理者の双方に影響を与える、安全に関する規定（第17条）は、簡略化された。措置の適切性の査定に対する危険基準を引き続き採用する一方で、措置の費用に対する検討が導入された。

（j）通知及び事前の調査（第18、19及び20条）

データの対象者の権利及び自由を損なうおそれが少ない処理作業の分類に対する通知からの免除（委員会からの提案）に加えて、処理作業を行うために、データ保護職員が任命され、それによって、データの対象者の権利及び自由を損なうおそれが少ないことが確保された場合に対して、通知義務の軽減が規定された。

データの対象者の権利及び自由に特有の危険をもたらすおそれのある処理作業の事前の調査は、監視機関（委員会の提案）又はデータ保護職員が監視機関と共同して行うことができる。国内法に従って、監視機関は、事前調査の後に、意見又は許諾を与えることができる。

通知及び調査に関する規定は、加盟国内で試みられてきた2つの種類の手続きが同等の効力を有するように調整を提供する。

(k) 第三国（第25及び26条）

欧州評議会は、委員会によって提案された包括的方針を承認した。すなわち、第三国に適切な保護レベルが存在しなければならないという原則、及び加盟国がその原則を固守することである。また、これに対して当分野でのECの政策は統一的に実施されることを確保するための規定が加えられた。欧州評議会は、保護レベルの査定及び義務の軽減に関して、検討されるべき局面を列挙した。

(l) 監視機関（第28条）

国内行政措置又は規則が作成される際には、必ず監視機関に助言を求めるべきことを規定した。監視機関の介入権は、暗示的に規定するとどめ、加盟国に対して、この分野において必要な独自の判断の余地を与えた。国境を越えるデータの流通に関する監視機関の間での協力に関する条文がより詳細に規定された。

(m) 委員会（第31条）

委員会へ実施権限を付与する必要がある第三国へのデータの移転に関して、欧州評議会は、1987年6月13日の決議87/373/EECの第2条に従って、手続き（a）を採択した。

(n) 最終条項（第32及び33条）

手作業のファイリングシステムを指令に従わせるための前述した移行措置の規定とは別に、指令を国内法に書き換えるための期限を指令の採択された日から3年に延長することが必要であるように思われる。

情報化社会の発展状況の文脈の中で、技術の進歩を考慮に入れるために、委員会は、特に音響及び画像形式の個人データの処理に対する指令の適用に関して調査し、定期的な報告書にその結果をまとめるものとする。

6 ワーキンググループメンバー名簿

ECOM

堀部 政男 主 査 一橋大学 法学部 教授
佐草 幸一 副主査 電子商取引実証推進協議会 主席研究員

委 員

相澤 良平 日本電気(株) EC 推進本部システム部 課長
赤羽 俊男 (株)東芝 コンセプトインテグレーション 開発部 CE 研究第 2 担当 グループ長
池田 忠且 (株)日立製作所 情報事業本部法務センター 部長代理
鈴木 康史 富士通(株) 法務知的財産権本部ビジネス支援部 ビジネスコンサルティング部 課長
巽 昭博 (財)金融情報システムセンター 調査企画部 調査役
田中 稔 日本信販(株) 審査本部審査指導部 マネージャー
塚原 宏 (株)さくら銀行 事務統括部 副主席
中込 孝 (株)アプラス 営業企画部 上席部長代理
余田 隆夫 日立クレジット(株) 経営企画室 部長代理
佐々木 祥仁 ユーシーカード(株) EC 事業部 アシスタントマネージャー
河崎 克也 (社)日本クレジット産業協会 会員部 主任
芦澤 武 三菱電機(株) マルチメディア事業推進プロジェクトグループ 主事

オブザーバー

東 昌弘 電子商取引実証推進協議会 モール構築技術検討WG 主査
高橋 基二 情報処理振興事業協会 技術センターコンピュータセキュリティ技術調査室室長補佐
関本 貢 (財)日本情報処理開発協会 情報セキュリティ対策室 課長

通商産業省

須藤 治 機械情報産業局情報処理システム開発課 課長補佐
田尻 貴裕 機械情報産業局情報処理システム開発課 企画係長

(順不同、敬称略)

以上