ISBN 978-4-89078-026-6
C3084

個人情報の安心安全な管理に向けた社会制度・基盤の研究会

報告書

平成 24 年 3 月

一般財団法人日本情報経済社会推進協会

個人情報の安心安全な管理に向けた社会制度・基盤の研究会は、近時、マイナンバー法案（行政手続における特定の個人を識別するための番号の利用等に関する法律案）や EU 個人データ保護規則案（個人データの取扱い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規則（一般的データ保護規則）の提案：Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)）等、個人情報に対して関心が高まっている中、個人情報に関する論点を明確化し、国際動向を踏まえつつ、あるべき姿等を検討することを目的として設置されたものである。

個人情報保護という考え方は、今でこそ広く知られるようになったが、ここに至る道程は決して楽なものとはいえなかった。私は、日本でプライバシーという言葉が知られるようになった 1960 年代初頭から、半世紀近くにわたり、プライバシー・個人情報のあり方について研究を重ねてきた。その中で、国、地方公共団体、民間部門における議論はもとより、国際的な議論にもかなりかかわってきた。現在の個人情報に関する制度等は、この研究と議論の積み重ねから少しずつ形成されてきた姿であり、今後も同様に繰返されることで進化していくことであろう。

本報告書はその議論の素材となるものであり、将来のプライバシー・個人情報のあり方について関心を持つ全ての人にとって有意義な資料となるはずである。本報告書では、近時の個人情報に関する論点を挙げ、国際的動向（アメリカ、ドイツ、イギリス、欧州委員会、OECD）について触れている。特に EU 一般データ保護規則案の翻訳資料は仮日本語訳ではあるが、かつて JIPDEC が事務局を担当していた電子商取引推進協議会（ECOM）のプライバシー問題検討ワーキンググループ（座長は筆者）において実施し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（Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data）の翻訳と同様、大変有益なものとなるだろう。本報告書が将来のプライバシー・個人情報に関わる活発な議論につながれば幸いである。

個人情報の安心安全な管理に向けた社会制度・基盤の研究会　顧問
一橋大学名誉教授　堀部政男

我が国においても情報ネットワークは既に社会基盤として、普段の個々人の生活において当たり前ものとして広く認識されるようになっている。一方で、絶え間なく報道されるプライバシー・個人情報に関わる事件は枚挙に暇がなく、社会的にも様々な議論がなされている。

個人情報の安心安全な管理に向けた社会制度・基盤の研究会においては、個人情報の適正な取扱いと保護に関する国内の議論にとどまらず、国外における社会制度や基盤の動向にも着目した先進的な調査研究が行われた。

個人情報の適正な取扱いと保護への取組は、一企業、一個人では対処できるようなものではなく、社会制度や基盤として対処していくことが必要な問題となっている。そのため、個人情報の安心安全な管理について研究会を設置して、個人情報について検討することは有意義であった。

国内においては、社会保障と税の一体改革の検討がなされ、当該分野において個人番号を用いることを定めたマイナンバー法案が本報告書の公表段階で審議がなされている段階にある。個人番号は、本人確認のための新たな社会基盤としての活用が期待されている。メディアなどの報道においても、共通番号という用語が用いられて紹介がなされているものの、個人番号の利用範囲が限定されていることから、本人確認としての一般的な利用が可能な共通番号としての利用は、現段階では想定されていない。

その一方で、本人確認や本人認証の重要性は、ネットワーク社会の進行とともにその重要性は高まるばかりである。そのため、諸外国における最新動向も踏まえた現状調査が求められてきたところである。

本研究会における具体的な論点整理については、本人確認・本人認証にかかわる論点、個人情報の保護に関わる論点、情報のコントロールにかかわる論点に分けて検討がなされている。また、諸外国における動向についても、アメリカ、ドイツ、イギリス、欧州委員会、OECD について、それぞれ、最新動向の紹介がなされている。

本報告書は、四回の研究会において検討対象となった論点を中心に、近時の問題として重要な論点をピックアップして整理したものであり、個人情報に関する論点を網羅しているわけではなく、未だ検討が十分ではない部分があるのも事実である。しかし、近時の話題や議論のための論点は十分に盛り込まれている。とりわけ、2012 年 1 月 25 日に公表された EU の個人データ保護規則案については､その全文翻訳とともに論点の整理も行われ、我が国において最も早く当該規則の研究を行った成果である。

個人情報の取扱いは、クラウド・コンピューティングに代表されるように、国境を越えて日々情報が流通する現状がある。そのため、国際的動向を注視することが不可欠となっており、我が国の対応について検討するにあたって、行政機関、民間事業者、そして個人による対応のあり方を考える上で、本研究会における検討と本報告書の成果が活用されることを期待したい。

個人情報の安心安全な管理に向けた社会制度・基盤の研究会　座長
慶應義塾大学　総合政策学部　准教授　新保　史生

目次

1　個人情報の安心安全な管理に向けた社会制度・基盤の研究会について

1.1　研究会の背景・目的

2011 年 10 月、一般財団法人日本情報経済社会推進協会（JIPDEC）、電子情報利活用推進部（DUPC）では「個人情報の安心安全な管理に向けた社会制度・基盤の研究会」を設置した。

現在、世界的に個人情報の保護やその活用に関して大きな過渡期を迎えている。近時の個人情報に関連する動向を概観してみると、我が国においては、社会保障・税に関わる番号制度の検討が開始され、2011 年 6 月 30 日には政府・与党社会保障改革検討本部により「社会保障・税番号大綱」[1]が決定され、2012 年 2 月 14 日には「行政手続における特定の個人を識別するための番号の利用等に関する法律案（通称「マイナンバー法案」）」[2]が閣議決定され、国会に提出された。

世界に目を向けると、EU では「EU 個人データ保護規則案（個人データの取扱い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規則（一般的データ保護規則）の提案：Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)）」が提案され、アメリカでは「サイバースペースにおける信頼できるアイデンティティのための国家戦略（The National Strategy for Trusted Identities in Cyberspace：NSTIC）」が打ち出され、「ネットワーク社会における消費者データプライバシー（Consumer Data Privacy in a Networked World）」において「消費者プライバシー権利章典（Consumer Privacy Bill of Rights）」が謳われている。ダボス会議では「パーソナル・データ再考プロジェクト（Rethinking Personal Data）」、OECD では「自然人のデジタル・アイデンティティ・マネジメント：インターネット経済における革新と信頼の付与－政府ポリシー立案者のための指針（Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers）」が公表されている。

個人情報に関して上記のような動きがあるのは、私たちの生活において、インターネットは今や電気、水道、ガス、電話に並ぶ社会基盤となり、なくてはならない存在であるとともに、今日、単なる社会インフラにとどまらず、人間活動が展開される実社会の陸、海、空（宇宙）と同様に現実とつながるひとつの空間（情報空間）として形成されつつあり、その重要性が急激に高まっているためである。昨今の情報通信ネットワークの発展から、

---

[1] "社会保障改革". 内閣官房. http://www.cas.go.jp/jp/seisaku/syakaihosyou/index.html,(accessed 2012-02-20).

[2] "行政手続における特定の個人を識別するための番号の利用等に関する法律案". 内閣官房国会提出法案. http://www.cas.go.jp/jp/houan/120214number/houan_riyu.pdf, (accessed 2012-02-20).

個人情報の量や多様性は、情報ビッグバンと呼ばれるように、世界的規模でまさに爆発的な増加を見せており、個人情報の経済的価値や社会的有用性は日に日に増している。我が国における一般生活の状況を見てみても、2011 年上半期にはスマートフォンの集荷台数が 1004 万台と携帯電話の出荷台数の半数を占めた [3]ことからわかる通り、個人の普段の生活により直結されるような情報の取り扱いが可能となることにより、多種多様な情報サービスが開発され、利用され、個人と情報空間との距離感は以前よりも更に密になっている。

一方で、個人の情報空間での活動が活発になればなるほど、自身に関する個人情報が多くの場所で保存・利用されることになり結果として自身では管理不能となっている現状がある。また、個人情報の価値が高まれば高まるほど、それに対する脅威やリスクは高まるため、世界的な大規模漏えいやサイバー犯罪等についても、注視しなければならない。

このような昨今の状況を背景として、個人情報の安心安全な管理に向けて、個人情報に関してあらためて見つめ直すことが必要であると考え、個人情報の保護と利用に関する論点を明確化し、あるべき姿などを検討することを目的として研究会を実施してきた。本報告書は研究会を通じて、取り上げてきた検討事項を整理し、取りまとめたものである。

1.2 研究会の体制

個人情報の安心安全な管理に向けた社会制度・基盤の研究会は、表 1-1 の体制で活動してきた。

表 1-1 研究会の体制

顧問	堀部　政男	一橋大学名誉教授
座長	新保　史生	慶応義塾大学
	稲垣　隆一	稲垣隆一法律事務所
	大山　永昭	東京工業大学
	長見　萬里野	日本消費者協会
	崎村　夏彦	野村総合研究所
	柴崎　亮介	東京大学
	米丸　恒治	神戸大学大学院
事務局	小林　正彦	JIPDEC
	亀田　繁	JIPDEC
	成海　洋	JIPDEC
	保木野　昌稔	JIPDEC
	野村　至	JIPDEC

[3] "2011 年度上期国内携帯電話端末出荷概況". 株式会社 MM 総研. http://www.m2ri.jp/newsreleases/main.php?id=010120111027500, (accessed 2012-02-20)

1.3 研究会の活動記録

個人情報の安心安全な管理に向けた社会制度・基盤の研究会は、平成 23 年度内に 4 回実施し、特別企画として、「個人認証環境セミナー」[4]を開催した（表 1-2, p.3, 参照）。

表 1-2 研究会の活動記録

活動日	活動項目	活動場所
2011-10-11	第 1 回　研究会	機械振興会館 6 階 6D-2
2011-11-29	第 2 回　研究会	機械振興会館 4 階 JIPDEC 第 3 会議室
2011-11-30	特別企画 個人認証環境セミナー	機械振興会館 6 階 6D-1, 2, 3
2012-01-20	第 3 回　研究会	六本木ファーストビル 1 階 JIPDEC 第 1 会議室
2012-03-09	第 4 回　研究会	六本木ファーストビル 1 階 JIPDEC 第 1 会議室

※ 個人認証環境セミナーでは Antonius Sommer 氏（TUV Informationstechnik GmbH, Managing Director）に、第 3 回研究会では高木浩光氏（独立行政法人産業技術総合研究所, 主任研究員）に招待講演をいただいた。

[4] "個人認証環境セミナー" JIPDEC. http://www.jipdec.or.jp/project/anshinkan/event/20111130.html.

2　個人情報の安心安全な管理に向けた社会制度・基盤の論点

2.1　論点の分類と整理

「個人情報の安心安全な管理に向けた社会制度・基盤」について検討するためには、まず、個人情報の保護とその活用に関して、現状としてどのような問題があるのか、論点を明らかにする必要がある。本章では、その個人情報に関わる論点の概要を述べる。論点については、「本人確認・本人認証に関わる論点」、「個人情報の保護に関わる論点」、「情報のコントロールに関わる論点」、の 3 つに分類、整理した。

「本人確認・本人認証に関わる論点」では、サービスごとに用意されている本人認証基盤の弊害、個人による ID・パスワード管理の限界がもたらすリスク、高い保証レベルに対応した電子的な本人確認の可能性について述べる。

「個人情報の保護に関わる論点」では、個人が事業者に提供する個人情報の最少化および個人が事業者に本当の個人情報を提供せずにサービスを受けられる機能の必要性、横断利用可能な識別子による名寄せのリスクについて述べる。

「情報のコントロールに関わる論点」では、事業者に提供した情報とそれに関連したサービスの情報について自分で把握すること、その情報を自分で利用できるようにすること、データ・ポータビリティや忘れてもらう機能の必要性について述べる。

2.1.1　本人確認・本人認証に関わる論点

今日、個人は多くのサービスを利用しているが、どのようなサービスのにおいても、常に正しい本人との対応を取りながら、作業を進めていく必要がある。言い換えれば、個人情報の安心安全な管理のためには、本人確認と本人認証という基本機能が十分その役割を果たすことが前提になっている。

本人確認と本人認証は極めて重要であるが、しかしながら、この本人確認と本人認証という言葉は、どの分野でも利用できる共通の定義があって、標準化された概念のもと広く使用されているわけではなく、各分野で部分的に定義したり、慣用的に使われているのが実態である。そのため、混乱を避けるためにも、本報告書における本人確認と本人認証については以下の意味で利用する。

本報告書での本人認証とは、「登録されている本人であると主張する人が、本当に登録されている本人であることを確認する行為」を意味する [5]。つまり「登録（registration）されている本人であると主張するAさん（要求者（claimant））に対して、たくさんの登録さ

[5] 本報告書での本人認証は"本人認証技術検討WG 報告書". 財団法人日本情報処理開発協会（JIPDEC）電子商取引実証推進協議会（ECOM）の定義をもとにしている。なお、本人認証の説明における英語表記は、本報告書での本人認証の意味をより詳しく伝える目的で併記している。

れた人の中からAさんを区別（登録されているn人の中から 1 人を識別（identification）する処理）し、本当にAさんであるかパスワード等を利用して確認（要求者が識別された 1 人であることを認証（authentication）する処理）する一連のプロセス」である。例えば、Aさんが国立国会図書館に入館する場合を考えてみる。入館管理端末に対してAさんは利用者登録済のボタンをタッチ（登録されている本人であると主張）し、利用者カードのバーコードを読み込ませることで、登録されているBさんでもなく、Cさんでもなく、Aさんであることを区別（識別処理）させ、Aさんしか知りえないパスワードを入力することで本当にAさんであることの確認（認証処理）を済ませ、入館する。このような一連のプロセスを本人認証とする。

本報告書での本人確認とは「当該主体に対して主体を明らかにする情報を入手し、用途や目的によって必要とされる真正性を満たしているかを確認する行為」を意味する[6]。例えば、Aさんが銀行口座を開設する時の本人確認を考えてみる。銀行員はAさん（主体（subject））に対して口座開設をする者であることを明らかにするため、Aさんの氏名、住所等（主体を明らかにする情報（information to identify））が記入された口座開設申込書を入手し、口座開設に必要な基準（保証レベル（level of assurance））の真正性を満たしているか確認する。必要な基準を満たしているかの真正性の確認方法として具体的には、運転免許証（evidence）を提出させ、運転免許証が偽造でないか確認（genuine check）し、申請書の項目と運転免許証の項目を照合（verification）し、運転免許証の顔写真を見て運転免許証の保持者と申請者が一致しているか確認（linking between bit and meat）する。このような確認作業の一連のプロセスを本人確認とする。「当該主体に対して主体を明らかにする情報を入手し、用途や目的によって必要とされる真正性を満たしているかを確認する行為」を本人確認とするので、本人確認において必ずしも氏名や住所等が必要というわけでない。例えば、本屋で本を予約したAさんが店頭で本を受け取る際の本人確認を考えてみる。本屋の店員はAさんに対して、Aさんが本の受取をする者であることを明らかにするためAさんから引換証（主体を明らかにする情報）を入手し、本を受け渡しするのに必要な基準（保証レベル）の真正性を満たしているかを確認（引換証が偽造ではないか等）する。このような一連のプロセスを本人確認とする。

(1) サービスごとに用意されている本人認証基盤

現在の多くのサービスは、個人がそのサービスを利用開始する際に自らの個人情報を事業者側に提供して会員登録をし、事業者から ID とパスワード（クレデンシャル）を取得し、そのクレデンシャルをもとに本人認証を行い、当該サービスを利用することが基本になっており、サービスごとに本人認証基盤が用意されている。これは様々

[6] 本報告書の本人確認は"ISO 24760-1"及び"ISO/IEC DIS 29115"の定義をもとにしている。なお、本人確認の説明における英語表記は、本報告書での本人確認の意味をより詳しく伝える目的で併記している。

な弊害を生じさせる。

弊害のひとつ目としてサービス利用開始の敬遠があげられる。サービスごとに本人認証基盤が用意されていると、個人はサービスの利用を始める前に登録プロセスを経なければならない。個人は新たなサービスを利用しようとする度に個人情報を入力する必要があり、この作業を面倒と感じて利用者登録を途中でやめてしまうことがある。2011 年に実施した株式会社野村総合研究所の調査 [7]によれば、ウェブサービスの利用者登録を途中でやめた経験がある人の割合は 9 割（図 2-1, p.7, 参照）であり、その原因として「入力項目の多かった」（61.4%）ことや「わざわざ入力するのが面倒だった」（44.2%）こと（図 2-2, p.7, 参照）をあげた者は多かった。

次に、サービスごとに用意された本人認証基盤は個人情報の漏えいリスクを増長させるという問題がある。サービスごとに本人認証基盤が用意されている場合、登録プロセスにおいてそれぞれのサービス事業者に対して個人情報を提供することになる。これは個人情報がサービス事業者それぞれに分散、保持されることになる。提供先である事業者が個人情報の管理が不十分な場合、そこから個人情報の漏えいにつながる可能性がある。

更に、多数のサービスに対して ID・パスワードを使い分ける必要性が生じるため、後述する 2.1.1(2)個人による ID・パスワード管理の限界につながり、パスワードの使いまわし等のセキュリティに対する脅威を増大させる。

---

[7] 安岡弘道, 伊藤智久, 冨田勝己. "事業者と生活者の ID 活用に関する実態調査 ～顧客に選ばれたサービス提供事業者との ID 連携がビジネスの鍵を握る～". NRI メディアフォーラム（野村総合研究所）. http://www.nri.co.jp/publicity/mediaforum/2012/pdf/forum170.pdf, (accessed 2012-02-20).

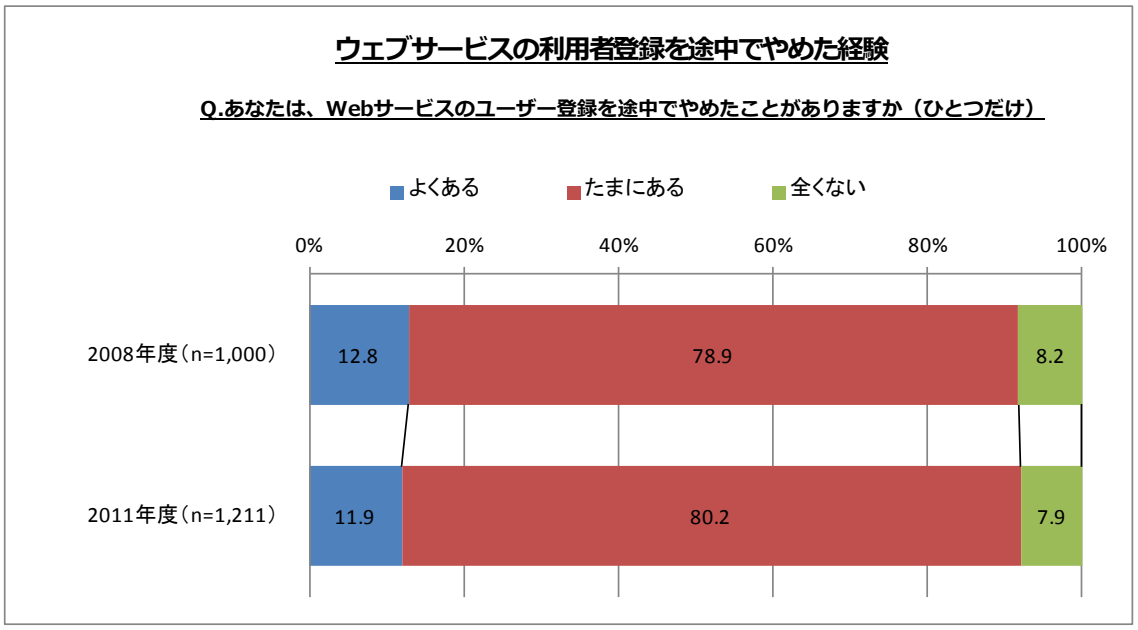


図 2-1 ウェブサービスの利用者登録を途中でやめた経験

出所：安岡弘道，伊藤智久，冨田勝己．"事業者と生活者の ID 活用に関する実態調査 ～顧客に選ばれたサービス提供事業者との ID 連携がビジネスの鍵を握る～". NRI メディアフォーラム（野村総合研究所））．

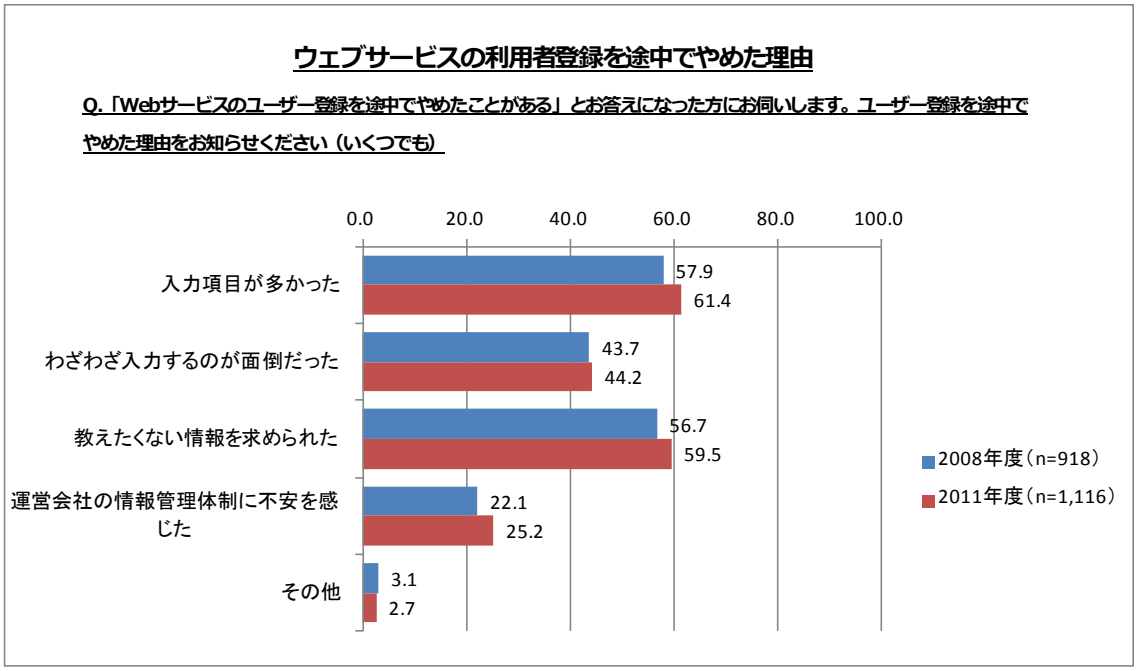


図 2-2 ウェブサービスの利用者登録を途中でやめた理由

出所：安岡弘道，伊藤智久，冨田勝己．"事業者と生活者の ID 活用に関する実態調査 ～顧客に選ばれたサービス提供事業者との ID 連携がビジネスの鍵を握る～". NRI メディアフォーラム（野村総合研究所）

(2) 個人によるID・パスワード管理の限界

個人にとってオンラインが身近になれば、多種多様なオンラインサービスを利用することになるが、一方で、サービスごとに本人認証基盤は用意されており、それぞれに対するクレデンシャルを個人は記憶しなければならず、それらの管理が個人の限界を超えてしまっている。

2011 年に実施された株式会社野村総合研究所の調査[7]によると、個人が ID とパスワードを使ってログインするサイト数の平均は 19.40（図 2-3, p.10, 参照）であった。個人は約 20 のサイトに対する ID とパスワードを保持していることになる。また、同調査による「ID やパスワードを管理する際、何組までなら確実に記憶することができるか」という問いに対して、平均記憶数は 3.15 という結果が得られている（図 2-7, p.10, 参照）。個人は約 3 組の ID とパスワードの組合せを記憶することができるが、それ以上になると記憶が曖昧になるということになる。すなわち、個人が利用する約 20 のサイトに対して、個人が確実に記憶できるクレデンシャルは 3 組ということになり、個人による ID とパスワード管理は限界を超えている現状にあると言える。

この限界は、個人が類推されやすいパスワードを設定したり、ひとつのIDとパスワードの組合せを複数のサービスで使いまわしたりするという状況を生み出している。2011 年に実施された独立行政法人情報処理推進機構の調査[8]では、パスワードを誕生日など推測されやすいものを避けて設定している割合は 48.4%にとどまり、半数以上は第三者に推測されやすいものを設定していることがわかる（図 2-5, p.11, 参照）。パソコン習熟度で最上級レベルである者においても、おおよそ 4 割は推測されやすいパスワードを使っていることになっている。また、2009 年に実施された株式会社野村総合研究所の調査[9]によれば、9 割以上の回答者がIDとパスワードを複数のサイトで使いまわしているという（図 2-6, p.12, 参照）。IDとパスワードの使いまわしの背景には、使いまわしが可能であるような本人認証基盤が、結果的に構築されているところにある。多くのサービスはIDとパスワードによる本人認証を用いており、かつIDにメールアドレスを指定していることが多い。IDとしてメールアドレスが使われるのは、メールアドレスに唯一性があり、メールは本人との連絡手段であるとともに、サービス利用開始の確認、パスワード失念時の対応手段としても使用できることが要因として考えられる。加えて、事業者はサービス利用者を増やすため、サービス利用開始の

---

[8] 独立行政法人情報処理推進機構. " 2011 年度 情報セキュリティの脅威に対する意識調査報告書".独立行政法人情報処理推進機構. http://www.ipa.go.jp/security/fy23/reports/ishiki/documents/2011_ishiki_report.pdf, (accessed 2012-02-20).

[9] 株式会社野村総合研究所 基盤ソリューション事業本部. "ID とパスワードに関する意識調査 分析レポート". 株式会社野村総合研究所. http://uni-id.nri.co.jp/resource/pdf/id_report_201002.pdf, (accessed 2012-02-20).

ハードルをできるだけ低くすることを目的に、7～8 割を超えるような高い割合で利用しているツール、つまりメールアドレスとパスワードの組合せを採用することも、その理由のひとつと考えられる。

個人のID・パスワード管理の限界である現状は、推測されやすいパスワードの設定やIDとパスワードの使いまわしを引き起こしているが、これはアカウント・クラックを含めた不正アクセスに対するリスクを高める。推測されやすいパスワードを設定することは不正アクセスを容易にし、IDとパスワードを使いまわすことは、ひとつのサービスのクレデンシャルがフィッシングや漏えい事故等により第三者に渡った場合、他の多くのサービスアカウントについても意図しない第三者からの脅威にさらされることになる。近時、不正アクセスは増加傾向[10]にあり、平成 24 年 2 月 21 日には不正アクセス禁止法の改正案が閣議決定されている。不正アクセスの手段は平成 20 年度までは「利用権者のパスワードの設定・管理の甘さにつけ込んだもの」が最も多く、平成 21 年度以降は「フィッシングサイトにより入手したもの」が大部分を占める[11]ようになっているが、依然として利用権者のパスワードの設定・管理の甘さにつけ込んだ不正アクセスは存在している。不正アクセスに対する脅威が高まる中、個人のID・パスワード管理の限界という状況は望ましくない。

10 警察庁. "不正アクセス禁止法の改正について". 警察庁. http://www.npa.go.jp/syokanhourei/kokkai/240221/sankou.pdf, (accessed 2012-02-24).
11 "平成 23 年度 警察白書 統計資料（不正アクセス行為に係る犯行の手口の内訳の推移）". 警察庁. http://www.npa.go.jp/hakusyo/h23/toukei/00/0-06.xls, (accessed 2012-02-24).

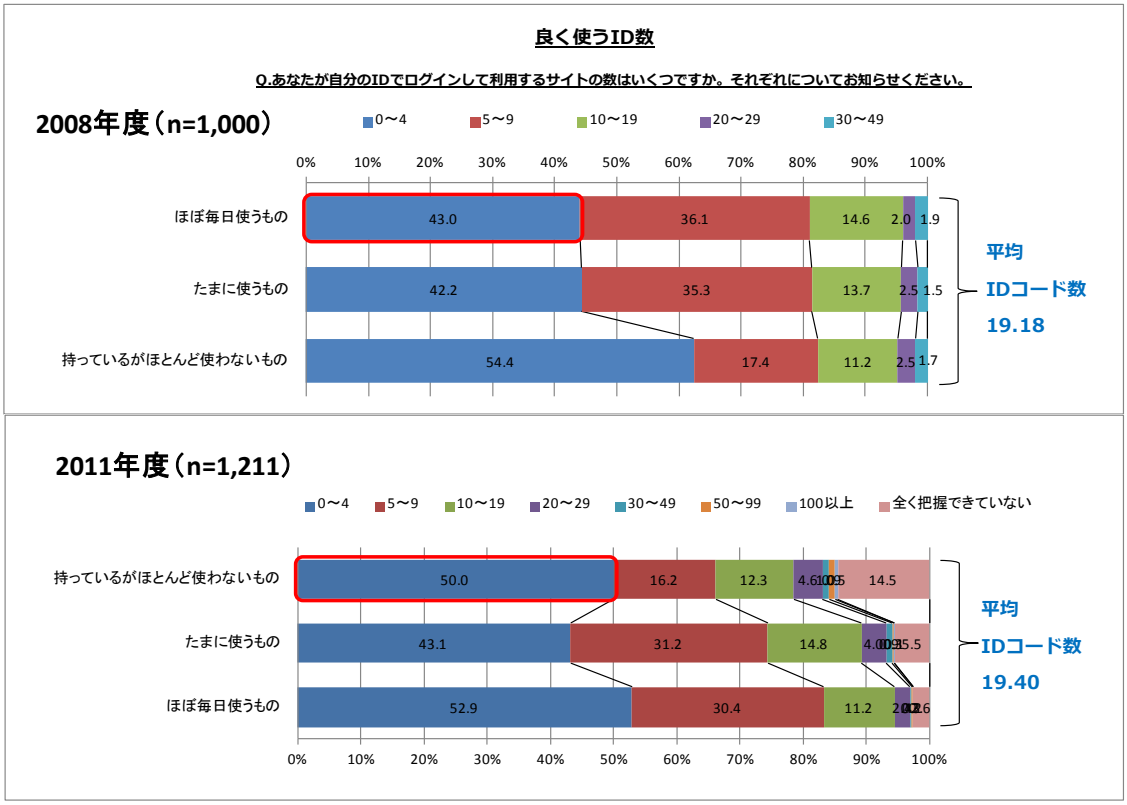


図 2-3 よく使う ID 数

出所：株式会社野村総合研究所 基盤ソリューション事業本部. "ID とパスワードに関する意識調査 分析レポート". 株式会社野村総合研究所.

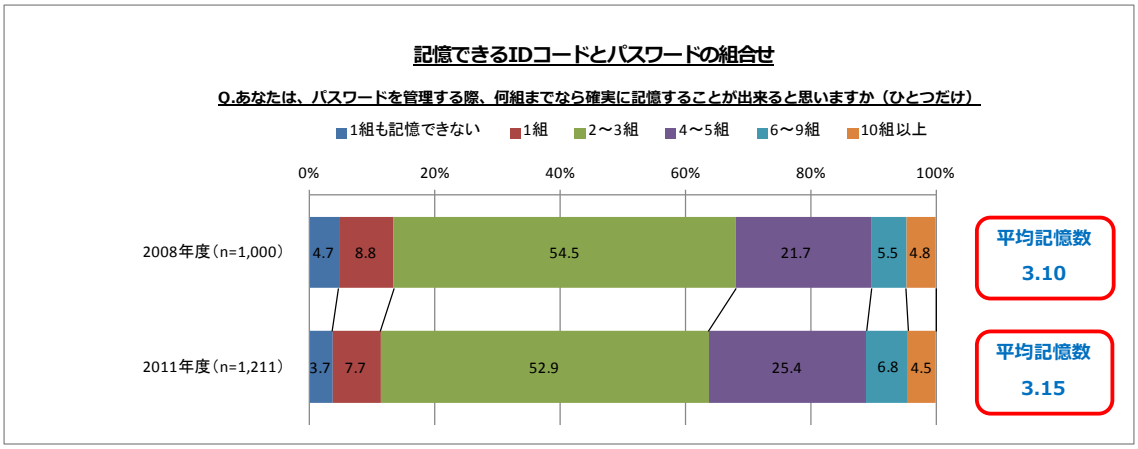
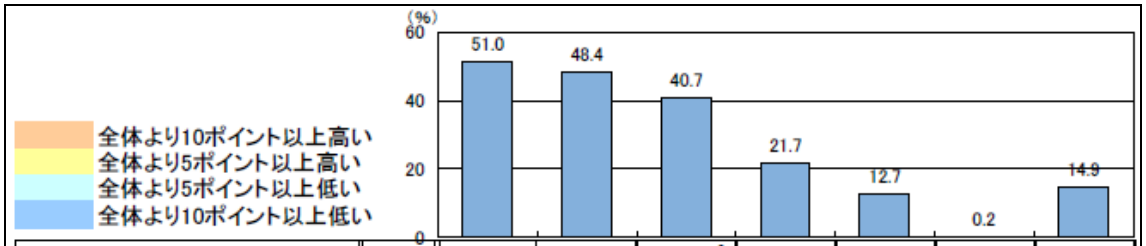


図 2-4 記憶できる ID コードとパスワードのの組合せ

出所：株式会社野村総合研究所 基盤ソリューション事業本部. "ID とパスワードに関する意識調査 分析レポート". 株式会社野村総合研究所



		n	パソコンのログインパスワードを設定している	パスワードは誕生日など推測されやすいものを避けて設定している	パスワードはわかりにくい文字列（8文字以上、記号含む）を設定している	サービス毎に異なるパスワードを設定している	パスワードは定期的に変更している	その他	あてはまるものはない
全体	全体	5240	51.0	48.4	40.7	21.7	12.7	0.2	14.9
年代別	15-19歳	388	55.2	41.8	40.7	13.7	6.2	0.3	14.7
	20-29歳	936	49.9	43.5	40.6	19.1	10.0	0.2	16.6
	30-39歳	1160	51.5	45.9	38.5	18.8	12.1	0.3	15.9
	40-49歳	1031	49.5	51.2	42.2	24.5	13.0	0.4	16.3
	50-59歳	973	52.7	51.8	38.6	23.2	15.3	0.1	14.0
	60-69歳	752	49.5	53.3	44.7	27.9	16.2	0.1	10.9
パソコン習熟度別	最上級レベル	555	58.7	60.2	55.0	32.3	21.1	0.5	10.5
	上級レベル	2459	51.7	49.9	43.2	23.5	12.7	0.2	13.9
	中級レベル	1957	48.3	45.3	36.2	17.9	10.7	0.2	15.9
	初級レベル	269	48.0	31.6	20.8	11.2	8.6	－	27.1

図 2-5 パスワードの設定方法

出所：独立行政法人情報処理推進機構. " 2011 年度 情報セキュリティの脅威に対する意識調査 報告書".独立行政法人情報処理推進機構.

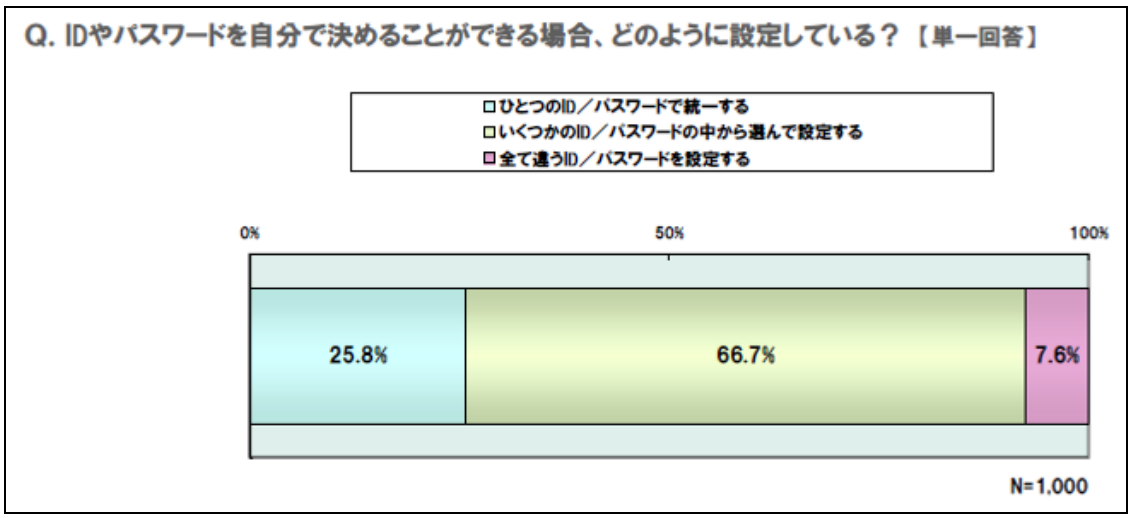


図 2-6 ID・パスワードの設定方法

出所：株式会社野村総合研究所 基盤ソリューション事業本部. インターネットで使用する ID とパスワードに関する意識調査.

(3) 高い保証レベルに対応した本人確認

現実の世界において、その者を明らかにし、必要な基準（保証レベル）に応じて、真正性を確認する本人確認は至る所で実施されている。例えば、簡単な講演会イベントでは主催者は会場に訪れた者に対して参加証を提示させることで参加者であることの真正性を確認する。学割商品であれば購入者に対して教育機関が発行した学生証を提示させて学生であることの真正性を確認する、銀行口座の開設であれば口座開設申請者に対して運転免許証等を提示させて口座開設が可能な者であることの真正性を確認する。本人確認は、それぞれの保証レベルに対応する確認手法を用いて実施される。

一方、インターネット上での本人確認はどのようになっているのか考えてみると、我が国において、高い保証レベルを要求するサービスを実現する際、そのレベルに対応する本人確認を実施するための主体の真正性を確認する電子ツールがないため問題が出てくる。高い保証レベルに対応する本人確認を実施する際の手法として、我が国には、公的個人認証サービスの電子証明書があるが、それはインターネットを利用した民間の商取引等において無制限に使うことができない。公的個人認証サービスの根拠法律である「電子署名に係る地方公共団体の認証業務に関する法律」では第 17 条において利用者の電子証明書が有効であるか否かを確認することができる主体について規定しているが、その主体を行政機関や裁判所等に限定している。また、公的個人認証サービスの電子証明書の適用範囲については各都道府県の認証局運用規程 [12]にて規

[12] "都道府県認証局の運営に関する情報". 公的個人認証サービス都道府県協議会. http://www.jpki.go.jp/ca/pref_rules.html, (accessed 2012-02-20)

定しているが、その適用範囲も限定されている [13]。ICカードタイプの運転免許証もあるが、運転免許証を保持していない者（保持できない者）は利用できないということになる。

誰であっても自由に利用でき、高い保証レベルを保ちつつ、民間で利用することのできる本人確認のための電子ツールがないことによるデメリットが考えられる。例えば、保険、金融、情報通信（携帯電話）といった分野のオンラインサービス展開や、青少年保護といったものである。

現時点においても、高い保証レベルに対応した本人確認が必要なオンラインサービスは展開されているが、それは高い保証レベルを維持するために非電子的な方法を用いたり、いくつもの手順を踏んだりして本人の真正性を確認しているものであり、手間とコストのかかる確認手法となっている。具体例として、携帯電話の購入や海外出張や臨時用途のための携帯電話レンタルサービスを挙げてみる。携帯電話の購入やレンタルは、インターネットによるオンライン申請を行うことによって、自宅まで携帯電話を宅配してもらうことができるが、その場合には本人確認のためにパスポート、運転免許証のコピーをFAXまたはメール等で別途携帯電話会社に送る必要がある [14]。

青少年保護の観点からも、本人確認は重要である。警察庁の資料（非出会い系サイトに起因する児童被害の事犯に係る調査分析について）[15]によれば、ソーシャル・ネットワーキング・サービス（SNS）を主とするコミュニティサイトに起因する児童被害の事犯が大幅に増加しているという。児童が被害に遭う要因としては、児童側がフィルタリング機能を無効化している等、様々考えられるが、青少年保護という目的のために必要な基準の本人確認が十分実施できていないということも、そのひとつとして見て取ることができる。警察庁の同資料によれば、被疑者の 46.6%は年齢も含めて身元（プロフィール）を詐称し、SNSに登録しているという。検挙事例として、48 歳の男性が年齢を詐称して男子高校生として女子児童に近づいたり、自己紹介サイトに登録している年齢の若い男性の画像を入手して、他のゲームサイトに登録している女子児童あてに同画像を送信するなどしてその男性になりすまして近づいたりということ

---

[13] 千葉県の例をあげると"千葉県認証局 運用規程"（http://www.jpki.go.jp/ca/pdf/12CPS.pdf）において「行政機関等及び裁判所で行う手続のオンライン申請・届出に係る電子署名」等に公的個人認証サービスの証明書の用途を限定している。また千葉県庁のホームページ"公的個人認証サービス Q&A"（http://www.pref.chiba.lg.jp/jousei/kojinninshou/qa.html）にて、公的個人認証サービスの電子証明書の用途は「行政機関等に対する電子申請等」及び「民間認証事業者が電子証明書を発行する場合の本人確認手段」に法律上限定されており、民間の商取引等に直接利用することはできない旨を記載している。

[14] "携帯電話の申込方法". GSM Rentafone Pty Ltd.日本支店. http://www.softbank-rental.jp/outbound/booking/, (accessed 2012-02-20).

[15] "非出会い系サイトに起因する児童被害の事犯に係る調査分析について". 警察庁. http://www.npa.go.jp/cyber/statics/h22/H22deai-bunseki.pdf, (accessed 2012-02-20).

が挙げられている。反対に児童側にも年齢を詐称している者もおり、利用者の年齢等属性に応じて利用可能なサービスを区別して設定するゾーンニングを乗り越えるということもある。青少年保護という目的のためには、現在の自己申告よりも高い保証レベルでの本人確認が必要であるが、それを実施するための容易な手段がない状況である。

2.1.2 個人情報の保護に関わる論点

(1) 個人情報の最少化

個人がサービスを受ける時、事業者に個人情報を提供し、それに基づいてサービスが提供されるが、この事業者に対して提供する個人情報を今よりも少なくできないかという論点がある。

情報社会が進む一方で、インターネット利用において不安を感じる者は多く、かつその中でも個人情報の保護に関して不安を感じている割合は非常に高い。総務省による平成 23 年 通信利用動向調査 [16]によれば、インターネット利用に対して不安を感じている人は 46%であるという（図 2-7, p.16, 参照）。その中でも個人情報の保護に不安があると答えたのは 71.6%にものぼり、不安のトップである（図 2-8, p.17, 参照）。

また、2008 年にMMD研究所が実施した「携帯サイトの会社概要・利用規約に関する実態調査」によれば、携帯サイト登録者を対象にサイト登録時の個人情報を入力する際に本当の情報を入力するかを調査したところ、「全部本当の情報を入力する」が 56.4%、「所々偽情報を入力する」が 41.7%、「全部偽の情報を登録する」が 1.9%という結果 [17]であった。前述の株式会社野村総合研究所の調査の、ウェブサービスの利用者登録を途中でやめた経験がある人の割合は 9 割であり、その原因のひとつとして「教えたくない情報を求められたこと」が半数以上ということを併せて考えると、本当の個人情報を相手に提供せずに、可能であれば個人情報を教えずにサービスを受けたい、とする者は少なくはないということが見て取れる。一般個人は、相手に教える個人情報は最少に、かつ、可能ならば個人情報を相手に教えずにサービスが受けられることを望んでいると言える。

個人情報を最少にするという点について考えてみたい。現在は少なくはなってきているが、必要以上に個人情報を入力させるようなサービスがある。個人情報の取得を

16 "平成 23 年 通信利用動向調査". 総務省. http://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201000_001.pdf, (accessed 2012-02-20).

17 "携帯サイトの会社概要・利用規約に関する実態調査". MMD 研究所. http://mmd.up-date.ne.jp/news/detail.php?news_id=211,

必要最低限にとどめることは、個人情報保護法では、第 15 条[18]および第 16 条[19]の利用目的に関わることである。利用目的は、単に抽象的、一般的に特定するのではなく、事業者が最終的にどのような目的で個人情報を利用するかを可能な限り具体的に特定することと考えられる。単に「事業活動に用いるため」、「提供するサービスの向上のため」、あるいは「マーケティング活動に用いるため」というように表現することは、利用目的を特定したことにはならない[20]。本人がその影響を予測できる程度に、利用及び提供の範囲をできる限り具体的に明記すべきである。しかしながら、この利用目的について、事業者はあいまいな記述を行い、必要以上に個人情報を取得、利用の範囲を拡大しているということがある。

次に、個人情報を相手に教えずにサービスが受けられることについて考えてみると、個人情報を相手に教えずにサービスを受けたいというニーズは個人側にはあり、そのようなサービスを実現させているものが現実にある。例えば、住所を教えたくないという人のための配送代行サービス、クレジットカード番号を教えたくないという人のための決済代行サービスといったものである。しかしながら、これらの代行サービスはすべてのオンラインサービスが対応しているわけではなく、オンラインサービスを提供する事業者側の意向によって決まるもので、個人側が情報を提供する、提供しないということを決めることはできない。また、名前、電話番号、メールアドレスなども事業者に知られたくない、入力したくないという人も 3 割から 5 割程度[21]おり（図

---

[18]（利用目的の特定）
第 15 条 個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。
2 個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

[19]（利用目的による制限）
第 16 条 個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。
2 個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。
3 前二項の規定は、次に掲げる場合については、適用しない。
一　法令に基づく場合
二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

[20] "個人情報保護マネジメントシステム要求事項の解説". 日本規格協会. p.74.

[21] 情報セキュリティに関するインターネット利用者意識 2006. NRI セキュアテクノロジー

2-9, p.18, および表 2-1, p. 19, 参照）、その場合、そもそもの会員登録時の代行から必要になってくるが、そのような個人情報の仲介サービスというものはない。しかしながら、事業者としても個人の身元がわからないことについての不安があり、何らかの問題が発生した時の連絡手段として個人情報を得ておきたいという理由や、代行業者が入ることにより手間や責任分界点で面倒がかかるということもある。

個人情報の最少化については、個人一人では解決できるものではなく、社会的な仕組みや制度として検討する必要があるものと考えられる。

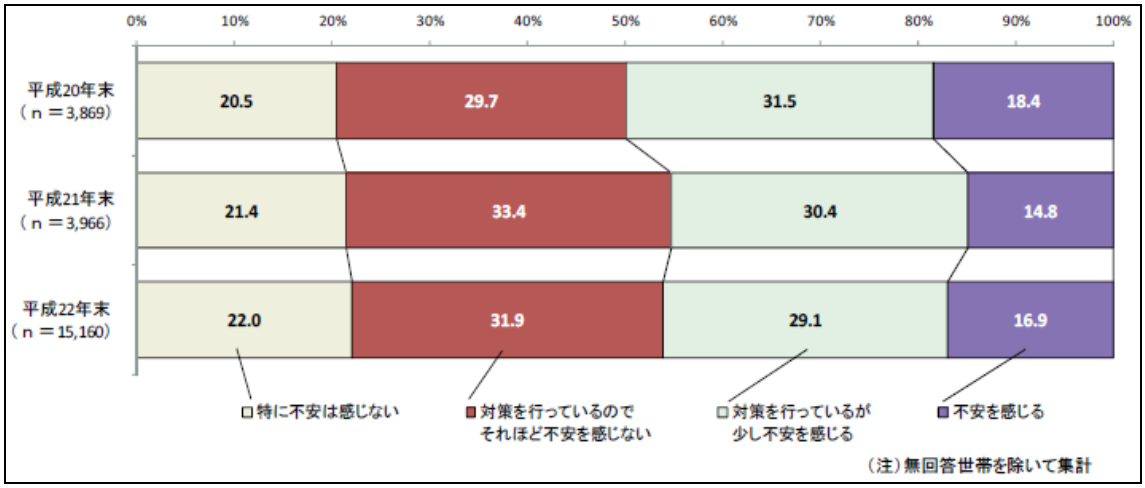


図 2-7 インターネット利用上の不安の有無の推移

出所："平成 23 年 通信利用動向調査". 総務省.

ズ株式会社. http://www.nri-secure.co.jp/news/2007/pdf/vol3-1.pdf, (accessed 2012-02-12)

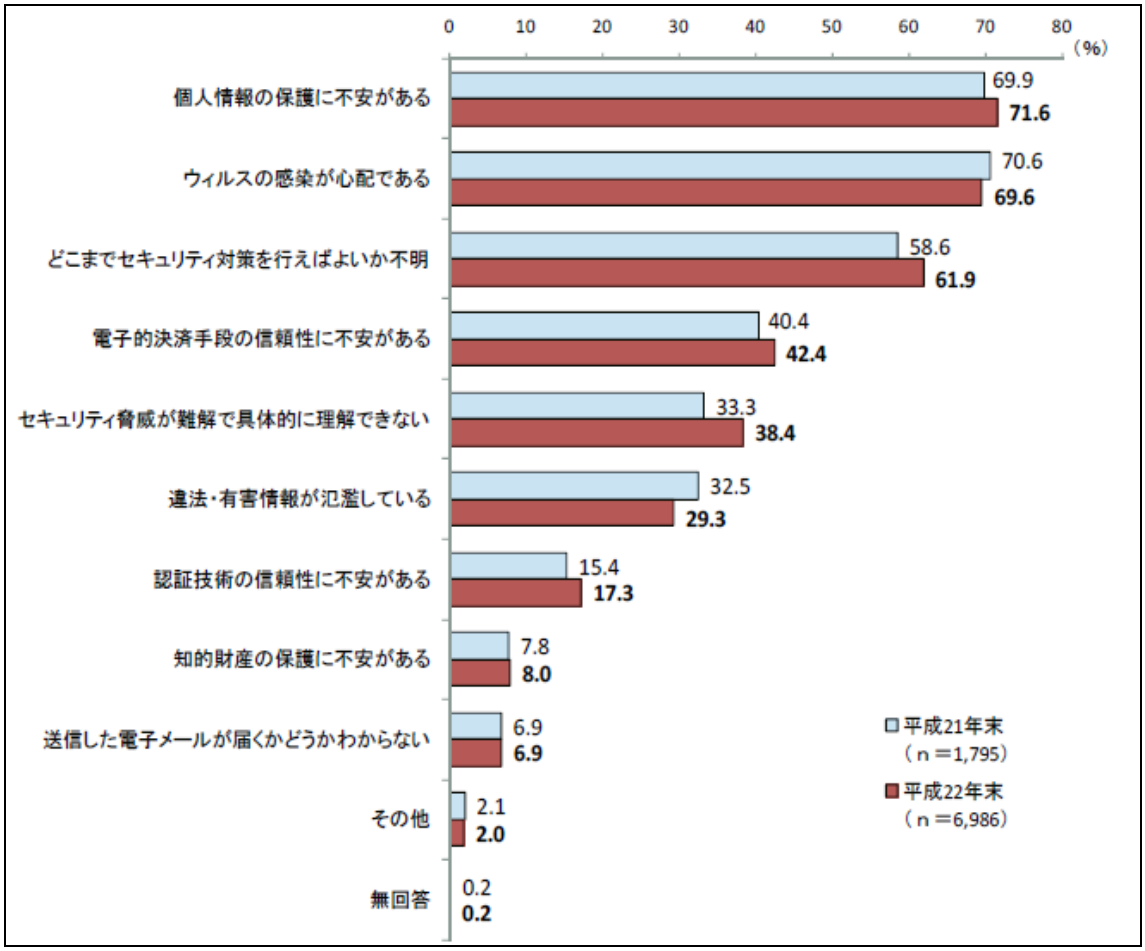


図 2-8 インターネット利用で感じる不安の内容

出所："平成 23 年 通信利用動向調査". 総務省.

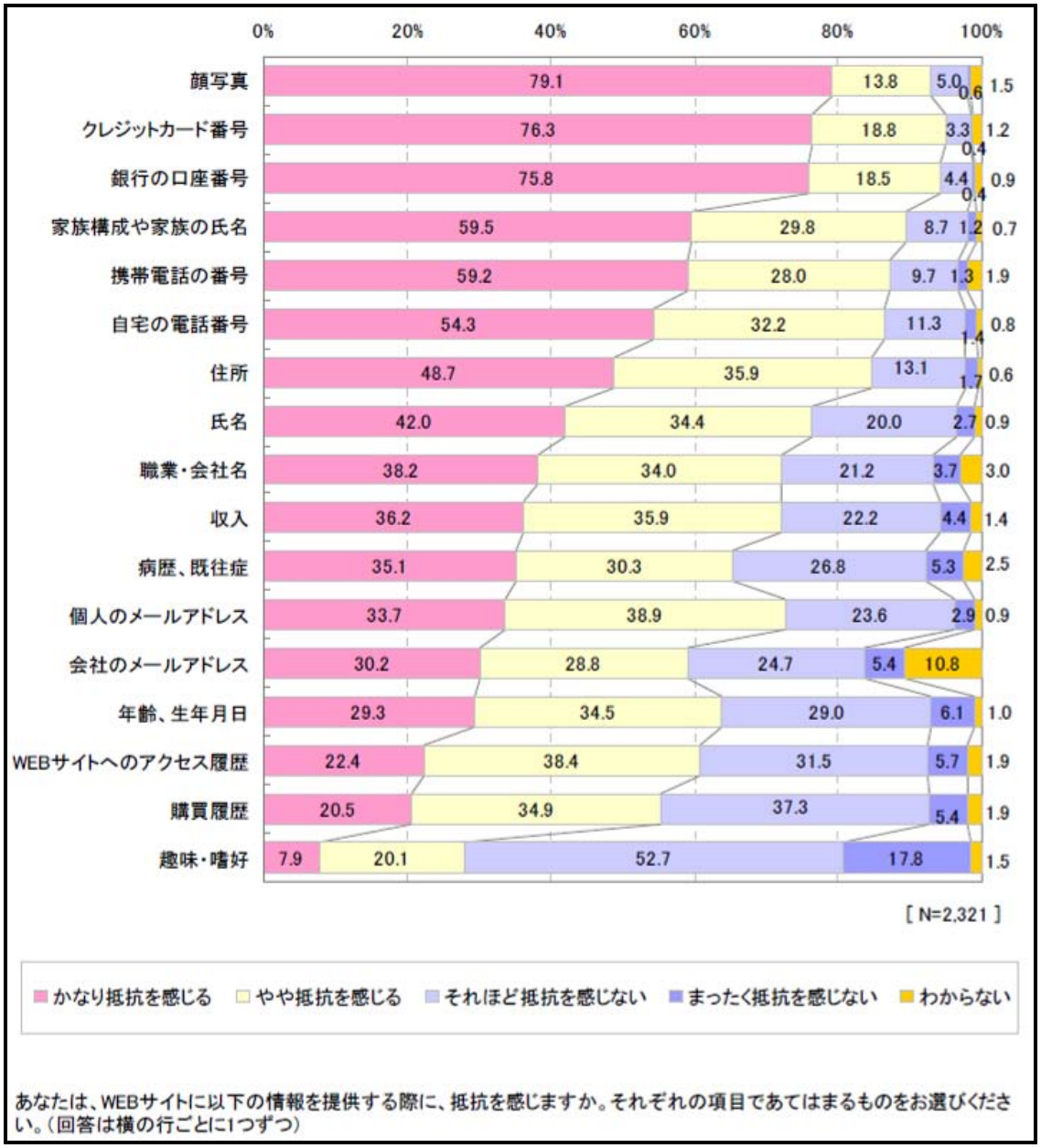


図 2-9 WEB サイトへ入力するのに抵抗を感じる情報

出所：情報セキュリティに関するインターネット利用者意識 2006. NRI セキュアテクノロジーズ株式会社.

表 2-1 オンラインで提供する情報

Q40 あなたは、インターネットでどのような情報を提供してもいいですか？

情報提供	はい		いいえ	わからない
	IPTS	日本		
名前/姓	86%	37%	50%	13%
年齢	90%	75%	17%	8%
国籍	87%	80%	13%	7%
身分証明書番号(保険証、パスポートなど)	13%	7%	82%	11%
住所	65%	19%	67%	14%
容姿(身長、体重など)	39%	36%	52%	12%
趣味やよくしていること	53%	75%	17%	8%
志向/意見	75%	69%	20%	11%
友人やよく会う人達、同好会の人達など	37%	22%	65%	13%
私が通常行く場所	27%	31%	54%	15%
mixi やフェイスブックのようなSNS に提供している情報	50%	41%	45%	14%
自分の写真	58%	7%	83%	10%
財務情報（収益、残高など）	9%	7%	83%	10%
医学情報（健康保険番号など）	7%	4%	87%	9%
銀行情報（銀行カード番号、アカウント番号など）	30%	4%	86%	10%
裁判の情報（前科情報・破産宣告の有無など）	5%	6%	85%	9%
バイオメトリックス情報（指紋、虹彩など）	4%	5%	85%	10%

出所："eID に対するセキュリティとプライバシに関するリスク認知と受容の調査報告". 独立行政法人情報処理推進機構セキュリティセンター. 2010 年.

(2) 横断利用可能な識別子の無制限な使用

横断利用可能な識別子が無制限に使用されることで、名寄せ等により個人情報が本人の意図しない形で利用される危険性が増すという論点がある。

この論点については内閣府の消費者委員会個人情報保護専門調査会 [22]において議論されており、具体例として携帯端末等の個体識別番号の問題があげられた。

携帯端末等の個体識別番号を利用した個人の行動追跡、名寄せ等が問題となっている。例えば、個体識別番号を用いた行動ターゲティング広告用のアクセス動向の追跡である。個体識別番号はそれぞれの携帯端末に振られている固有の番号であり、その保持者である個人との結びつきが非常に強く、また携帯端末はいつも持ち運び、様々な状況で携帯端末を利用することから個人の行動や生活と密着している。その個体識別番号を用いて、複数のサービス間で個人の利用履歴と紐づけて取集し、広告に利用するということがあった。横断利用可能な識別子を用いた名寄せの問題は携帯端末の個体識別番号に限らず、他の識別子でも同様に起きうるものである。

2.1.3 情報のコントロールに関わる論点

(1) 自己情報の管理

個人にとって、自分に関する情報を把握し、それら情報の訂正、利用停止、抹消、移行を難なくできるようにできないかという論点がある。

インターネットでのサービスを利用する機会が多くなればなるほど、個人は自分に関わる情報が把握しきれなくなる。例えば、これまでどのサービスに登録したか失念することがある。かろうじて記憶していたとしても、どの種類の情報を、どういった内容で、どの条件で、いつ提供したか、記憶しておくことは至難の業である。この自分の情報を把握できないことの弊害は、引っ越しをしたり、携帯電話番号の変更、メールアドレスの変更、クレジットカードの変更、口座の乗り換えをしたりしたときに現れてくる。どのサービスに、どのメールアドレスを教えたのか、あのサービスは、前の住所のままなのか、個人が確認するためにはそのサービスに問い合わせをしなければならない。仮にサービスにどういった情報が登録されているかわかっていたとしても、一人平均約 20 サイト利用している現状（図 2-3, p. 10, 参照）では、自分の状況の変化に応じて、それらすべてを変更することは労力がかかる。

---

[22] "第 5 回 個人情報保護専門調査会 議事録". 内閣府. http://www.cao.go.jp/consumer/history/01/kabusoshiki/kojin/005/gijiroku/index.html, (accessed 2012-02-20).

また、これからの情報社会で大きな問題になると考えられるのが「ロック・イン」である。あるサービスを利用し始めると、それから人々は逃れられなくなるという問題である。自分のデータへのアクセスが容易であることや、そのデータを自分で使えるようにすること、そしてあるサービス・プロバイダーから別のサービス・プロバイダーへとデータの移転ができるような、データのポータビリティを確保することが必要と考えられる。

3　個人情報の安心安全な管理に向けた社会制度・基盤の動向

3.1　アメリカ

アメリカにおける個人情報関連の動向を見たとき特徴的なのはパーソナル・データの利用、プライバシー保護、デジタル・アイデンティ・マネジメント、トラスト・フレームワークなどに関して包括的な戦略を打ち出していることである。アメリカの動向については、株式会社野村総合研究所の崎村夏彦氏の資料[23]と併せて参照いただきたい。

3.1.1　アメリカのID戦略（NSTIC）

(1)　インターネットをもはやツールではなくサイバースペースと見る

アメリカでは「サイバースペースにおける信頼できるアイデンティティのための国家戦略（The National Strategy for Trusted Identities in Cyberspace：NSTIC）」という国内向けの政策を打ち出した。

アメリカでは、インターネットを、陸、海、空、宇宙と同じように考え、サイバー空間という形でとらえている。我が国ではインターネットをツールとしてとらえることが多いが、それとは大きく異なっている。

このサイバースペースでは、データが非常に大きな意味を持ってきている。情報が経済成長に大きな意味を持つということは、様々なところで聞かれることである。例えば、ビッグデータという言葉であったり、ダボス会議の「パーソナル・データ再考プロジェクト（Rethinking Personal Data）」では、パーソナル・データ・エコシステムという言葉で紹介している。そのパーソナル・データ再考プロジェクトでは「パーソナル・データはインターネットの新たな石油であり、デジタルワールドの新たな通貨である（Parsonal data is the new oil of the Internet and the new currency of the digital world）」と述べている。パーソナル・データはデジタル世界（サイバースペース）での通貨としてみることができる。現実にインターネットのサービスにおいても、ID 連携をもとに、データの流通と連携をさせるサービスが増えてきている。この経済的価値の高いパーソナル・データをすみやかに、錯誤なく、流通できる仕組みを持つ国、企業が競争優位に立つことになると考えられる。しかしながら、パーソナル・データを流通や連携するためには、取引先の信頼やプライバシーの保護を含め、現実の貨幣と同様、セキュリティや信頼の確保が必須である。安心して取引ができなければ、

[23] 崎村夏彦. "アメリカの OITF、NSTIC と OpenID ファウンデーションの活動". 個人認証環境セミナー. http://www.jipdec.or.jp/project/anshinkan/doc/20111130/02.pdf, (accessed 2012-02-20).

流通はできない。

(2) サイバースペースを快適で安全な空間に

サイバー犯罪はアメリカのみならず、世界的に増加傾向にある。例えば、ID詐欺はEUの主要な犯罪である。McAfeeは情報経済のセキュリティに関する調査レポート「無防備な経済：重要情報の保護（Unsecured Economies: Protecting Vital Information）」を発表[24]したが、企業の知的財産損害は1兆ドルを超えると推定した。Europolの報告によれば、イギリスだけの被害で700億ユーロであり、EU全体の年間被害額がギリシャとポルトガルの救済費用と同額にもなる。

このように、サイバースペースで犯罪行為が横行している状況に対して、各国や各企業は防衛のためにそれぞれ自前で対策を行っている。しかしながら、この自前の防衛というのは、その防衛の程度が誰にもわからず、本当に安全性が担保されているかが不明なため、安心して自由な取引を行うことはできない。反対に、防衛の程度がわかると、取引に必要な安心の程度がわかるため、自由な取引が実現でき、経済の規模も広がり、その成長が加速されると考えられる。そのような環境を支える政策がNSTICである。

(3) NSTICの4つのガイディング・プリンシプル

NSTICには4つのガイディング・プリンシプルがある。

1番目は、コスト効果的で使いやすいこと

2番目は、セキュアかつ回復力に富むこと

3番目は、互換性に富むこと

4番目は、プライバシーを強化し、自発的な参加であること

である。

(a) コスト効果的で使いやすい、セキュアかつ回復力に富む、互換性に富む

コスト効果的で使いやすいこととは、経済学的に言うところの「パレート効率的」であることを意味する。パレート効率的ではない状態というは、誰の効用も下げずに誰かの効用を改善し得る非効率的な状態である。その意味において、パレード効率的である状態ということは重要である。完全競争市場が成立すればパレード効率的であるという事はよく知られているが、完全競争市場は、一種の聖杯であり、絶対に手に入れることができない状態ではある。しかしながら、完全競争市場を阻害

[24] "無防備な経済：重要情報の保護". マカフィー株式会社. http://www.mcafee.com/japan/security/unsecured_economies09.asp, (accessed 2012-02-20)

している要因を排除することで完全競争市場に近づくことはできる。完全競争市場を阻害しているものとは、①不透明性（情報の非対称性）、②安全でない環境に起因する摩擦コスト、③市場細分化と選択肢の欠如である。政策的にはこれら完全競争市場の阻害をどのようになくしていくかと言うのが重要であり、NSTIC の要である。

① 不透明性（情報の非対称性）

不透明性とは、参加者間の情報の調整のことをいう。経済学でいう、レモン市場をなくすことである。レモン市場とは、財やサービスの品質が買い手にとって未知であるために、不良品ばかりが出回ってしまう市場のことである。レモンとは、アメリカの俗語で質の悪い中古車を意味しており、レモン市場とは、中古車のように実際に購入してみなければ、真の品質を知ることができない財が取引されている市場を例えている。

これに対する対処法として監査人の設置がある。実際の中古車を例に考えた場合、監査人は、中古車を監査し、レーティングを付け、これは問題なく走行できる、無事故である、ということを保証する。その保証した情報を消費者の側に提供し、監査を基礎とした認定とその結果を公表することで、不透明性を解消する。

サイバー空間というのは、このレモン市場の問題に瀕していると言える。例えば「私は田中です」という主張をネットの向こうにいる人に信じさせることは至難の業である。主張者の情報量というのは受信者の情報量を凌駕しており、受領者の方は殆ど情報がない状態である。その時に監査を基礎にした認定と結果の公表というのは非常に重要になる。この監査による認定と公表の仕組みをトラスト・フレームワークと言う。アメリカで政府が認定しているトラスト・フレームワークの例としては、OIX、Kantara Initiative、InCommons の提供しているトラスト・フレームワークがある。

② 安全でない環境に起因する摩擦コスト

安全でない環境に起因する摩擦コストは完全市場を阻害させる。安全でない環境とは、昔であれば、シルクロードで絹を運んでいる途中に山賊に襲われたり、インド洋でスパイスを運んでいる途中に海賊に襲われたりすることである。近時は、空賊ということもある。安全でない環境ではコストが莫大になってしまい本来あるべきよりもはるかに少ない取引しか行っていないため経済成長が阻害される。これら安全でない環境を整備することによって、多くの取引が行われる。

サイバー空間の安全環境の状況を考えると、今は全くと言っていいほど整備されていない状況にある。これを安心安全な環境にすることによってサイバー空間での取引が更に加速することになる。

サイバー空間における対処法として、空間内の参加者の管理（アイデンティティの管理）が必要になる。相手が誰か正しく認識できると、情報の非対称性が緩和され、参加者が怪しいかどうかがわかる。

このアイデンティティの管理を強化するはじめの手順として、最も利用されているが「最も弱い輪」であるパスワードの排除がある。次に、社会保障番号（Social Security Number）を本人確認に使用するような非合理的慣習の排除がある。社会保障番号による本人確認は非合理的である。社会保障番号は、様々な所で使われている情報で、容易に知りえる情報である。このような容易に知りえる情報を利用した場合は安心安全な本人確認ができないため、社会保障番号を本人確認に使用するような非合理的慣習を排除していくという取り組みが必要となる。

更にガバナンスサイドの対処として、不届き者に対する処罰とその実施能力や強制能力をいかに担当していくかというのが制度的には重要となる。

そして、トラスト・フレームワークの設計も重要と考えられる。すなわち、参加者が遵守する技術的および運用的標準を定める、監査・認定・公表を通じて透明性を確保する、法執行メカニズム、調停機構の設計である。法執行メカニズムにおいて、アメリカが特徴的なのが「私的法律」としての「契約」を通じて既存の法執行インフラにリンクするという手段がとられることが多いことである。なぜ、私的法律を用いるかというと、法律の制定がサイバー空間の進度に間に合わないからである。情報技術の進化は急速であり、法律が対応できなくなってしまうことが多い。したがって、現在の法律体制に依存しきっていては対応ができなくなるのである。既存の法執行は最終的なところでは利用するが、それ以前に私的法律としての契約で現実に合わせて行くようにしていくのである。もう一つの観点として、契約だとジュリスディクションを超えられるところにある。サイバー空間というのは、いとも簡単にジュリスディクションを超えてしまう。

安全でない環境に起因する摩擦コストをなくすことは、すなわち、セキュアかつ回復力に富むことであり、それは NSTIC のガイディング・プリンシプルのひとつである。

③　市場の細分化と選択肢の欠如

市場の細分化と選択肢の欠如は完全競争市場の阻害要因である。市場の細分化と選択肢の欠如に関しては「細分化させないことの重要性」と「提供財の多様性と自由な選択を確保することの重要性」の 2 点をまず考慮しなければならない。

細分化させないことの重要性とは何か。

完全競争市場に近づけるためには、できるだけ健全な競争がそこにあることが鍵になる。ところが互換性を持たないテクノロジーによって市場の細分化、サイロ化、囲い込み化が行われていくと、それは非競争的となる。そのサイロ化された中では

提供者が一社しかいない状態になり競争が起きなくなる。したがって、ある一定性の互換性を持たせる、あるいは強制させて複数の提供者がそこに同一の市場の中に存在するようにするという事が、非常に重要になる。この重要性が、「細分化させないことの重要性」である

提供財の多様性と自由な選択を確保することの重要性とは何か。

個人、企業、政府は求めるものが異なっており、多種多様な財が提供されて、それを自由に選択できることが重要である。そのためには自由な参入の確保と要件のゆるさが必要である。競争を細分化されないことが重要であるとして、ある基準やスタンダードを決めて厳しく管理すると、例え複数社から成り立っている市場でも、まったく同一の物しか提供されないようになる。多様な思考を持っている人々や企業のニーズを満たすことができなくなるので、自由な参入の確保と要件のゆるさを確保することが重要である。この重要性が、「提供財の多様性と自由な選択を確保することの重要性」である。

市場の細分化と選択肢の欠如を排除することは、すなわち、互換性に富むことであり、それは NSTIC のガイディング・プリンシプルのひとつである。

(b) プライバシーを強化し自発的な参加であること

サイバースペースにおいて、安心して取引ができる透明性があり、安全な環境の中、適切な経済活動ができるだけでは十分ではない。基本的な幸福追求権としてプライバシーが確保されているという事も非常に重要である。

そういった意味では、自分かどういう情報をどういう相手に提供するかという事の自由性というのは完全に確保されなければならず、実名で活動するのか、あるいは仮名で活動するのかということも確保されている必要がある。

このプライバシーを強化のために、アメリカでは、Fair Information Practice Principles（FIPPs）の 8 箇条を掲げており、これに合致させるようとしている。

1 番目は「透明性（Transparency）」、
2 番目は「個人の参画（Individual Participation）」、
3 番目は「目的の特定（Purpose Specification）」、
4 番目は「データの最小化（Data Minimization）」、
5 番目は「利用の制限（Use Limitation）」、
6 番目は「データの品質と完全性（Data Quality and Integrity）」、
7 番目は「セキュリティ（Security）」、
8 番目が「説明責任と監査（Accountability and Auditing）」
これらを満たしていていなければいけないというベースラインを示している。

3.1.2 オープン・アイデンティティ・トラスト・フレームワーク（OITF）

3.1.1 で述べた NSTIC が指している、トラスト・フレームワークとは、オープン・アイデンティティ・トラスト・フレームワーク（Open Identity Trust Framework：OITF）をいう。この OITF は個人とアメリカ政府間で信頼して相手と情報のやり取りを行うためのフレームワークである。

トラスト・フレームワークというのは新しい概念ではなく、またアメリカに限るものでもなく、これまでいくつもあった。例えば、PKI のブリッジ CA（Bridge CA）、アイデントラスト（identrust）等である。OITF がそられと異なっているのは、アメリカ政府自身が定めたということ、大きな原則を規定し、多くの関係者が参入しやすいものにしていることがあげられる。

(1) OITFの原則

OITF とは「Principles of Openness」を満たしているトラスト・フレームワークをいう。Principles of Openness とは以下のような内容である。

表 3-1 Principles of Openness

合法的であること	Lawfulness
契約書/報告書等の公開	Open reporting and publication
独立したオンブズマンの設置	Ombudsmen
裏契約の排除と情報公開	Anti-circumvention and open disclosure
非差別	Non-discrimination
相互連携互換性	Interoperability
バージョン作成の公開	Open versioning
参加者の取り込み	Participant involvement
個人情報保護	Data Protection
説明責任	Accountability
監査可能性	Auditability
是正機会の提供	Redress

(2) OITFの仕組み

OITF の仕組みについては図 3-1（p.28）を参照いただきたい。まず、ポリシー策定者が関係者の守るべき原則を定める。このポリシー策定者に当たるのは、ICAM（Identity, Credential, & Access Management）である。そして、そのポリシーをトラスト・フレームワーク・プロバイダーが実際に監査可能な基準を定めトラスト・フレームワークを提供す

る。トラスト・フレームワーク・プロバイダーには、OIX、Kantara Initiative、InCommons があたる。トラスト・フレームワーク・プロバイダーは監査可能な基準に従って、監査人を認定する。認定監査人は、実際に情報を提供するアイデンティティ・プロバイダーについて監査する。Kantara Initiativ ではデロイトを認定監査人としている。情報を受け取る人の監査もするが、受け取る側が政府の場合、ポリシー策定者が政府なので、政府が監査する。

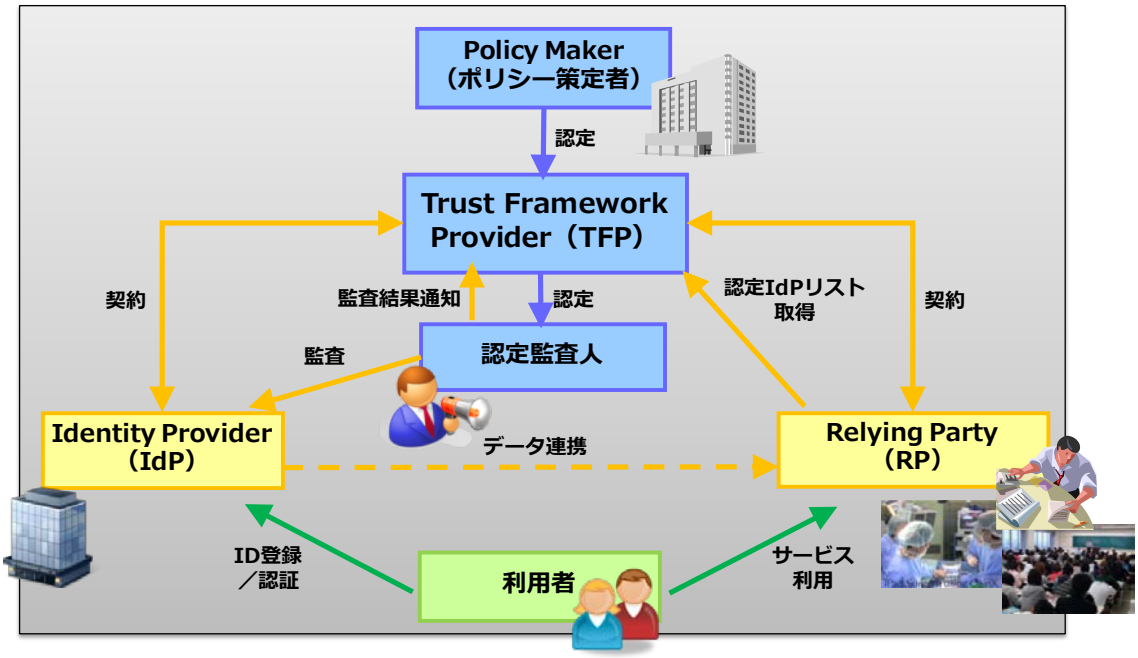


図 3-1 Open Identity Trust Framework の仕組み

出所：崎村夏彦. "アメリカの OITF、NSTIC と OpenID ファウンデーションの活動". 個人認証環境セミナー

3.2 ドイツ

ドイツにおける個人情報関連の動向を見たとき特徴的なのは、新身分証明書（neue Personalausweis：nPA）とDe-Mail法制である。ドイツの動向については、本研究会で実施した個人認証環境セミナーでのAntonius Sommer氏の資料[25]および神戸大学大学院の米丸恒治教授の資料[26, 27]に詳しく記載されているので参照いただきたい。

3.2.1 新身分証明書(nPA)

(1) ドイツの新身分証明書の動向

欧州各国はこれまで各国独自で身分証明書の法制を展開してきており、身分証明書の電子化への対応も、各国で異なる展開をしてきた。例えば、スペインでは「Documento nacional de identidad（DNI）[28]」があり、イタリアでは「Carta d'Identità Elettronica（CIE）[29]」がある。それとともに、欧州統合の動きの中で、電子的な身分証明について共通化を図る動向が出てきており、実証実験等のプロジェクト[30]が進められてきている。

ドイツでは、紙の時代から続く身分証明書法および身分証明書の電子化における他の先進国の成果を踏まえつつ、新身分証明書（neue Personalausweis）を導入した。新身分証明書は「身分証明書と電子的身元確認に関する法律（Gesetz über Personalausweise und den elektronischen Identitätsnachweis)」（以下、身分証法という）が2009年6月18日公布、2010年11月1日施行という法制定過程の後、発行された。この新身分証明書法制は電子的な官民共用の本人確認環境の実現を図る一方で、個人情報の保護の観点から、自己コントロールに関する事項も規定している。これはドイツ政府が電子政府政策「電子政府2.0」に基づいて新身分証明書を重要施策と

---

[25] Antonius Sommer. "The recent trend of the personal authentication environment and "eID" in Germany". http://www.jipdec.or.jp/project/anshinkan/doc/20111130/01_a.pdf, (accessed 2012-02-20)

[26] 米丸恒治. "論説・解説/電子取引における認証と個人情報保護 -ドイツ新電子身分証明書における認証と個人情報保護技術-". Law and Technology. 2011, No.51, p. 54-63.

[27] 米丸恒治. "ドイツ De-Mail サービス法の成立 -安全で信頼性のある次世代通信基盤法制としてのドイツ版電子私書箱法制-". 行政&情報システム. 2011年6月号, p. 30-35.

[28] "Portal Oficial sobre el DNI electrónico". Dirección General de la Policía. http://www.dnielectronico.es/, (accessed 2012-02-20)

[29] "Carta d'identità elettronica". Ministero dell'Interno. http://www.interno.it/mininterno/export/sites/default/it/temi/servizi_demografici/scheda_006.html, (accessed 2012-02-20)

[30] "Stork". https://www.eid-stork.eu/, (accessed 2012-02-20)

してきただけでなく、安心安全で利便性の高い次世代電子社会基盤の整備を進める戦略をとってきたためである。

(2) 新身分証明書の概要

新身分証明書は、IC チップが埋め込まれたクレジットカードサイズのプラスチック製のカードであり、16 歳以上のドイツ市民は義務として所有する。新身分証明書の表面には顔写真、氏名、生年月日、出生地等が記載され、裏面には、目の色、身長、居住地等が記載される。新身分証明書にはいくつか特徴的な機能がある。

① eID-Funktion（電子的本人確認機能）

新身分証明書の特徴的な機能のひとつとして電子的本人確認機能（eID-Funktion）がある。eID-FunktionのeIDとはelectronic Identityを意味するものであり、eID-Funktionは、新身分証明書のICチップに記録されている電子的な本人証明用データを用いて、電子的な行政手続のみならず、民間サービス等[31]において本人であることを証明する機能[32]である。このeID-Funktionを利用するかどうかは本人の選択となる（身分証法 10 条）。このeID-Functionの本人確認は、署名法上の認証事業者による署名用の証明書の発行でも利用することが認められており、次に述べる電子署名の利用促進の効果が期待されている。

② Unterschriftsfunktion（電子署名機能）

新身分証明書の所有者は、手書きのサインと法的に同等の適格電子署名（Qualifizierte elektronische Signatur：QES）の署名機能を利用することができる。ドイツにおいては、日本における公的個人認証サービスのような公的認証サービス・署名カード発行のサービスはなく、認証業務は民間の認定認証事業者等により供給されることとされている。しかし、電子署名用署名カードや、カードリーダの普及が進まず、電子署名の利用も普及してこなかった。そのため、ドイツ政府は、身分証を国民に義務的カードとして保有させ、そのカード上で、電子署名用の証明書を利用した適格電子署名の機能を普及させることを目指している。

③ elektronischen Reisepass（電子的旅券機能）

新身分証明書は、EU 域内における電子旅券として、パスポートに代わる国際的な旅行用文書としても利用することが可能である。新身分証明書の IC チップには

31 新身分証明書のアプリケーションの例 http://www.ccepa.de/onlineanwendungen/

32 "Die neuen Funktionen". Das Bundesministerium des Innern. http://www.personalausweisportal.de/DE/Die_neuen_Funktionen/die_neuen_funktionen_node.html, (accessed 2012-02-20)

生体情報が記録されており、偽造・改ざんの検証も可能である。なお、新身分証明書に生体情報（指紋情報）を記録するのは、義務的なものではなく、その保有者の選択に委ねられている。新身分証明書の印刷面には、所有者の顔写真が印刷され、従来の身分証明書と同様に、本人確認に利用されるほか、本人の選択により、2 指の指紋を、チップに記録することが可能な設計となっている。写真とともに、指紋の生体情報をチップに記録することにより、安全で信頼性ある本人確認を可能とする。なお、これらの生体情報を含む情報の読み取りは、法制上も規制されており、技術的には読取端末認証を受けた端末のみが読み取ることのできる。

(3) 新身分証明書における個人情報保護の特徴

新身分証明書を官民共用とするにあたっての個人情報保護については注目すべき点がある。

① 新身分証明書のシリアルナンバーの利用制限

ドイツでは、個人情報保護の観点から国民の統一 ID による識別やプロファイリング（個人情報の名寄せ等による）を防止する観点が重視されている。例えば、新身分証明書に記載されているシリアルナンバー（Ausweisnummer）は、カード発行機関の管理およびカードの失効手続等には利用されるが、共通 ID 等としてその他の目的でのデータの共用や名寄せ等に利用することは禁止されている（身分証法 20 条 3 項）。

② 個人情報の提供先の確認と提供する個人情報の選択

新身分証明書では eID-Funktion として電子的な本人確認や新身分証明書に記録された個人情報を行政や民間事業者に提供することができる。しかしながら、eID-Funktion を利用できる主体を厳格に限定している。

新身分証明書に記録されている個人情報を利用（eID-Funktionを利用）するためには、事業者等は、まず、連邦総務庁の審査機関（Vergabestelle für Berechtigungszertifikate (VfB) im Bundesverwaltungsamt）の審査を受ける必要がある。事業者等の実施する業務において、どの種類の個人情報を必要とするのかについての審査を受け、事業者等の個人情報の保護管理の現状について審査される [33]。この審査に合格することで事業者等はeID-Funktionの利用を許可され、カード内にある個人情報の許された項目のみ読み出すことができる。この仕組みは、証明証プロバイダー（Zertifikateanbieter）から事業者等に対して発行される権限証

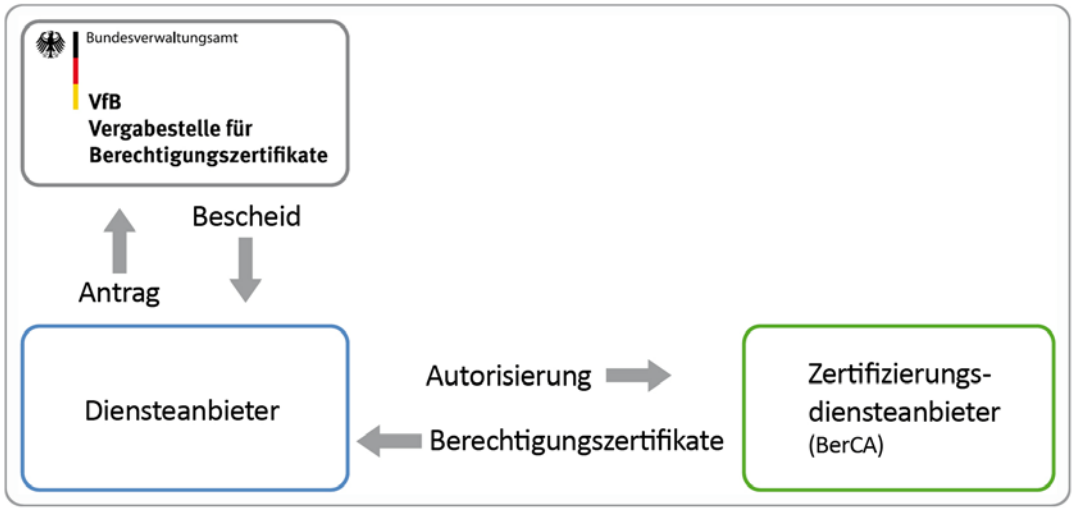
[33] "Berechtigungszertifikate". Bundesministerium des Innern. http://www.personalausweisportal.de/DE/Diensteanbieter_werden/Anwendungsbeispiele/Zugang_mit_Pseudonym/pseudonym_node.html,

明書（Berechtigungszertifikate）を用いて実現される（図 3-2, p. 32, 参照）。

この権限証明書は、ユーザーと事業者等とのオンライン通信の際に利用される。権限証明書は電子署名に利用される公開鍵証明書と同様の技術が使われ、偽造等検知が可能なように発行者による電子署名が付されている。ユーザーは権限証明書をもとに、事業者が本当に実在しているのか、個人情報保護対策を実施している信頼性があるのか確認し、権限証明書に記載されている個人情報保護監督機関も確認しながら、どの範囲の個人情報を相手方に送信するかどうかを自らが選択することができる。相手方事業者等を確認したユーザーは、パスワードをカード読取端末に入力して、カード内に格納されている個人情報を相手方事業者等に送信することになる。

こうした、事業者等の権限証明書を確認することで、当該証明書の事業者の存在や正当性、個人情報の保護管理状態が知ることができ、提供する個人情報の範囲が選択できることは、新身分証明書の特徴的な個人情報保護技術の一つであるといえる。

図 3-2 権限証明書入手プロセス



出所："Berechtigungszertifikate". Bundesministerium des Innern. http://www.personalausweisportal.de/DE/Diensteanbieter_werden/Berechtigungszertifikate/berechtigungszertifikate_node.html,

③ シュードニム・アクセス（Pseudonymer Zugang）

新身分証明書では、相手方に伝える個人情報を最少化するために、例えばオンラインフォーラムやチャットルームへの参加（Teilnahme an Online-Foren in Chat-Rooms）等、住所や氏名などを必要としないような場面においては、真正な個人情報に代えて、サービスごとに固有なものとして生成される「仮名符号（法令用語上は、サービス・カード固有識別符号（dienste- und kartenspezifisches

Kennzeichen))」（身分証法 2 条 5 項）を利用して厳密な相手確認が可能なようにしている。仮名符号は新身分証明書中の秘密データと権限証明書の事業者符号から一方向的に計算される符号として生成され、官民を問わず許可されたサービス事業者ごとに分離された仮名符号がもちいられる。この仮名符号は、これまでの各国の電子的身分証明書には見られない点である。

④　個人情報保護監察官（Datenschutzaufsichtsbehörde）の権限

事業者等による個人情報の濫用が疑われる場合には、個人情報保護監察官は権限証明書を取り消すことができる（身分証法 21 条 5 項）。これによって事業者等の規律をコントロールすることができる。

ドイツでは国民を識別するための統一番号（共通番号）ｍｐ考え方がとられていないだけでなく、さらに仮名（Pseudonym） を使うことができる技術的な仕組みも新身分証明書に導入している。身分証明というと、一般的には、実名による本人確認をイメージするが、ドイツにおいては、すでに電子署名法（1997 年制定「デジタル署名法」）上でも、仮名による署名を法制化してきており、個人情報保護の観点から、個人情報の最少化や仮名の利用を法制度上認めてきた。

3.2.2 De-Mail

De-Mail とは、ドイツの情報通信サービスのひとつである。De-Mail はインターネット上において市民、行政、事業者間で法的電子文書の交換を可能にする。De-Mail は行政と企業との通信コスト削減を目的として検討が始められ、民間企業とドイツ政府の協力によって実現したものである。2011 年 5 月 3 日に De-Mail 法（Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften – De-Mail-Gesetz）が制定され、De-Mail というサービスの法的根拠として機能している。

(1) De-Mail法の背景

現在の電子メールには様々な問題点がある。問題点の一つ目として、相手方の不確実性がある。メールアドレスだけでは相手が実際誰であるか確認することができない。二つ目として、暗号通信が普及していないことがある。電子メールの暗号化には S/MIME があるが、一般ユーザーの間ではほとんど利用されていない。三つ目として本当に送信したこと、そして確かに受信したことを証明するような、書留、配達証明、本人限定受け取りサービスなどに相当するものがない。これらの問題点が、電子メールが法的な効果が認められる通信基盤として利用することができない要因となってい

る。

De-Mail 法は、この問題に対して、インターネット上での電子メール等による通信の安全性や信頼性の欠如を法制度的に克服して、法的にも確実な通信基盤を作り上げようとするものである。

(2) De-Mail法の概要

安心安全でかつ信頼のある通信基盤を構築するための根拠となる De-Mail 法は以下のような特徴を持つ。

(a) De-Mailサービス・プロバイダーの認定制度（17 条）

De-Mailのサービス・プロバイダーは、一般のメールサービスと同様、民間の事業者等が中心的な事業主体（例えば、GMX[34]、WEB.DE[35]、FP/Mentana[36]、Telekom[37]）であるが、De-Mailサービスのサービス全体の信頼性を担保するため、サービス・プロバイダーの認定制度を設けている [38]。連邦内務省傘下の連邦情報技術セキュリティ庁（BSI）は、サービス・プロバイダーに対して安全性、機能性、相互運用性、プライバシー保護（Sicherheit, Funktionalität, Interoperabilität, Datenschutz）等について審査する。

(b) 本人確認に基づくDe-Mailアカウント開設（3 条）

何人も、De-Mail の申請をすることができるが、それに対し、De-Mail サービス・プロバイダーは、申請者の本人確認を確実に行わなければならない（De-Mail 法 3 条）。

De-Mail サービス･プロバイダーは、自然人の場合は、氏名、出生地、生年月日および住所、法人や公的機関の場合は、その名称、登記番号、事務所所在地ならびに代表者等の情報を収集して、ユーザーの同定のための情報として利用・保存する（De-Mail 法 3 条 2 項）。

---

[34] "De-Mail". GMX Internet Services, Inc. http://service.gmx.net/de/cgi/g.fcgi/products/de-mail,
[35] "De-Mail mit WEB.DE" WEB.DE . https://produkte.web.de/de-mail/?mc=produkte@home@navi.produkte@home@de-mail,
[36] "Wir sind akkreditierter Anbieter für De-Mail bei Unternehmen und Behörden und Privatpersonen" Francotyp-Postalia. http://www.francotyp.de/de-mail/index.php,
[37] "De-Mail von der Telekom für Geschäftskunden". Deutsche Telekom AG. http://www.telekom.de/de-mail/,
[38] "Informationen zur Zulassung von De-Mail-Anbietern". Beauftragte der Bundesregierung für Informationstechnik. http://www.cio.bund.de/DE/Innovative-Vorhaben/De-Mail/Akkreditierung/akkreditierung_node.html,

サービス・プロバイダーは収集した情報の真正性を確認する（De-Mail 法 3 条 3 項）。自然人については、前述の新身分証明書のように所持人の写真付きの有効な公的証明書や、適格電子署名の利用によって確認する。法人については、商業登記簿や協同組合登記簿または同等の公的登記簿等を用いる。

De-Mail サービス･プロバイダーは、De-Mail の中心的なサービスとして、ユーザーに De-Mail アドレス（メインアドレス（Hauptadresse））を与える。メインアドレスには、自然人や法人の名を含める（De-Mail 法 5 条 1 項 2 号及び 3 号）。De-Mail サービス・プロバイダーは自然人ユーザーより求めがあった場合には、仮名（pseudonyme）のアドレスを提供することができる。仮名のアドレスは、第三者が仮名であることを認識できるようにする必要がある（De-Mail 法 5 条 2 項）。

ドイツでは、個人情報保護の観点から、仮名の利用が極めて重視されており、De-Mail 法でも、仮名の利用が制度的に保障されている。

(c) De-Mail アカウントへの安全なログインの確保（4 条）

De-Mail サービス･プロバイダーはユーザーに対して、De-Mail アカウントへの安全なログインを可能にし、それにより個々のサービスへのログインを可能にする必要がある（De-Mail 法 4 条）。ログインには、互いに独立した 2 つのセキュリティ手段により不正な使用に対して保護されているか、携帯電話の SMS 経由のワンタイムパスワードなど秘密の一回性及び秘密性が守られる方法を用いる。ユーザーが求めれば、ID とパスワードの組合せによる方式の利用も認められるが、eID の利用を含む 2 方式の提供がプロパイダの義務とされている。

(d) 安全で信頼性がある確実な私書箱・配送サービスの提供（5 条）

De-Mail サービス･プロバイダーはユーザーに対して、電子メッセージのための安全な電子私書箱及び安全な配送サービスを提供する必要がある（De-Mail 法 5 条 1 項）。電子私書箱及び配送サービスでは、メッセージの秘密性、完全性、真正性を保証する必要がある（De-Mail 法 5 条 3 項）。

De-Mai サービス・プロバイダーは、送信者の求めがあれば、メッセージの送信証明を行う（De-Mail 法 5 条 7 項）。また、送信者の求めがあれば、メッセージが受信者の私書箱に届いたことの証明が行われる。これは送信者の De-Mail サービス・プロバイダー及び受信者の De-Mail サービス・プロバイダーが協力して行う。受信者の De-Mail サービス・プロバイダーは、受信証明書を発行する（De-Mail 法 5 条 8 項）。さらに当該メッセージを受信者が読み出した証明も行うことができる（De-Mail 法 5 条 9 項）。

(e)　アイデンティティ証明サービス（6 条）

De-Mail サービス・プロバイダーは、De-Mail 法 3 条に基づいて提供されたアイデンティティ・データを第三者に対し、De-Mail サービス・プロバイダーの適格署名を付して提供するアイデンティティ証明サービスを行うことができる（De-Mail 法 6 条 1 項）。このサービスは De-Mail サービス・プロバイダーの必須のサービスではなく、オプションサービスである。

(f)　ドキュメント・ストレージ・サービス（7 条）

De-Mail サービス・プロバイダーは、ドキュメント・ストレージ・サービスもオプションとして提供することができる（De-Mail 法 7 条）。De-Mail サービス・プロバイダーはドキュメント・ストレージ・サービスを提供する場合、ユーザーの電子データを長期間安全に保管し、秘密性、完全性、可用性も担保しなければならない。その際、全文書の暗号化を施さなければならない。

(g)　De-Mailサービスを支える各種の義務

De-Mail 法では、De-Mail サービス・プロバイダーに対して次のような義務を課している。

①　説明・情報提供義務（9 条）

De-Mail サービス・プロバイダーは、ユーザーに対して、De-Mail の法的効果等についての説明義務を負う（De-Mail 法 9 条）。De-Mail サービス・プロバイダーは、ユーザーが各種サービスを初めて利用する前にその法律効果等、重要事項を説明しなければならない。

②　業務の停止に関わる義務（11 条）

De-Mail サービス・プロバイダーはその業務を停止する場合、速やかに主務官庁に届け出る必要があり、その場合は、別の De-Mail サービス・プロバイダーに業務を引き継がれるよう配慮する必要がある。また、De-Mail サービス・プロバイダーは関係するユーザーに対して、業務の停止及び他の De-Mail サービス・プロバイダーにより引き継がれることを速やかに伝達する必要がある（De-Mail 法 11 条 1 項）。

業務を引き継ぐ De-Mail サービス・プロバイダーがいない場合、De-Mail サービス・プロバイダーは、ユーザーへの通知時点から少なくとも 3 ヶ月間はデータを読み出し可能な状態にしておく必要がある（De-Mail 法 11 条 2 項）。さらに、引き継ぐ De-Mail サービス・プロバイダーがいないときは、監督庁（BSI）がデータ等を引き継ぐこととされている（De-Mail 法 11 条 3 項）。

(h)　情報請求権（16 条）

De-Mail サービス・プロバイダーは、第三者に対してユーザーの氏名と住所に関する情報を、一定の条件のもと提供する（De-Mail 法 16 条 1 項）。その条件は、6 要件定められており、例えば、ユーザーへの法的請求権の行使に必要であること、請求が権利濫用にあたらないこと、個別事案においてユーザー保護の利益より勝ることなどがある。

3.3 イギリス

イギリスにおける個人情報関連の動向を見たとき特徴的なのは、国民の身分証明書としてのIDカードを配付することを中止し、民間が発行するアイデンティティの利用を考えていること [39]と、事業者が持つ個人に関する情報を事業者にとどませるのではなく、個人側にも使わせるようにしているmidataという試みの 2 点があげられる。以下、その 2 点について記述する

3.3.1 イギリスのアイデンティティ政策

(1) イギリスのIDカード法の成立と国民ID登録簿の導入

2004 年 4 月にイギリスでは「IDカードに関する立法（Legislation on Identity Cards)」[40]を発表し、2003 年 11 月 23 日にIDカード法案（Identity Card Bill）が議会に提出された。

この 2 年後、2006 年 3 月 30 日にIDカード法（Identity Card Act）[41]が成立した。IDカード法では、国民ID登録簿（NIR：National Identity Register）の構築と、その登録簿に基づいてIDカードを発行することを定めたものである。

IDカードおよび国民ID登録簿の導入の背景には、テロ対策があった。イギリス内でIDカードに対する議論が本格化したのは、2001 年 9 月 11 日のアメリカ同時多発テロ事件がひとつの契機と考えられる。内務大臣（Home Secretary）のデビッド・ブランケット（David Blunkett）は権利カード（entitlement cards）について触れて [42]おり、後に権利カードからIDカードへ（Identity Cards）と名称が変更 [43]され、検討が進めら

---

[39] イギリスの ID カードおよびアイデンティティ政策について、国立国会図書館の岡久慶氏の記事("【短信:イギリス】 2006年ID カード法－国民情報の総合管理". 外国の立法. 2006年, 第 229 号, p. 158-163, http://www.ndl.go.jp/jp/data/publication/legis/229/ 022907.pdf. および "英国 2006 年 ID カード法". 外国の立法. 2006 年, 第 230 号, p. 28-71, http://www.ndl.go.jp/jp/data/publication/legis/230/023002.pdf.）と株式会社国際社会経済研究所の小泉雄介氏の資料（"海外における国民 ID の動向 ～日本での導入に向けた考察～". 国際社会経済研究所. http://www.i-ise.com/jp/report/NationalID20101213.PDF.pdf）を参考文献としてあげておく。

[40] Home Office."Legislation on Identity Cards". TSO Online Bookshop. http://www.archive2.official-documents.co.uk/document/cm61/6178/6178.pdf, (accessed 2012-02-20)

[41] " Identity Card Act 2006". legislation.gov. http://www.legislation.gov.uk/ukpga/2006/15/contents/enacted, (accessed 2012-02-20)

[42] "A question of identity". BBC News. http://news.bbc.co.uk/2/hi/uk_news/1562427.stm, (accessed 2012-02-20)

[43] "Identity Cards A Summary of Findings from the Consultation Exercise on

れてきた。

IDカードおよび国民ID登録簿といった国家的アイデンティティ計画の目的は、組織犯罪やテロの予防（help the prevention of organised crime and terrorism）はもちろんのこと、市民の身元情報の証明手段の提供（provide a reliable way of checking the identity of people in positions of trust）、EU圏内の移動の簡易化（make travelling in Europe easier）、インターネット上を含んだ金融商品の申請や金融取引の安全な手段の提供（provide a secure way of applying for financial products and making financial transactions, including those made over the internet）、年齢証明の安全で便利な手段の提供（offer a secure and convenient way of proving your age）、公共サービスや公共利益享受のための適格性の確認と不正利用の削減（help to confirm your eligibility for public services and benefits – and reduce fraud relating to these services and benefits）、イギリスへの不法移民の削減と不法就労の取り締まり（help combat illegal working and reduce illegal immigration to the UK）等を狙っていた [44]。

2009年11月30日、マンチェスターにてIDカードの発行を開始した。発行手数料は30ポンド [45]であった。IDカードの発行は、イギリス内に居住する16歳以上が対象であり、取得は任意であった [46]。このIDカードは、身分証明書として、また、EU域内パスポートとして機能するものだった。カード券面には氏名、顔写真、生年月日、性別、国籍、出生地等の情報が記載される [47]。IDカードの申請方法は次のとおりである [48]。

Entitlement Cards and Identity Fraud". p. 45. Home Office. http://www.archive2.official-documents.co.uk/document/cm60/6019/6019.pdf, (accessed 2012-02-20)

[44] "What are the benefits of the National Identity Scheme?". Home Office. http://www.identitycards.gov.uk/benefits-glance.asp, (現在は閲覧不可 accessed 2007-11-01)

[45] Home office. "Announcements Identity card launch date announced". the National Archives. http://webarchive.nationalarchives.gov.uk/20100303180447/http://ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1329.htm

[46] Directgov. "Who can get the cards?". the National Archives. http://tna.europarchive.org/20100413151427/http://idsmart.direct.gov.uk/who-can-get-the-card.html

[47] Directgov. "About the cards". the National Archives. http://tna.europarchive.org/20100413151427/http://idsmart.direct.gov.uk/about-the-card.html

[48] Directgov. "How to apply for an identity card". the National Archives. http://tna.europarchive.org/20100413151427/http://idsmart.direct.gov.uk/how-to-apply.html, (accessed 2012-02-20)

① IDカード発行希望者が申請書一式（application pack）をアイデンティティおよびパスポートサービス（IPS：Identity and Passport Service）に電話またオンラインで請求する。
② IDカード発行希望者は送られてきた申込書を同封のガイダンス冊子をもとに記入する。
③ IDカード発行希望者はナショナル・アイデンティティ・サービス・カスタマー・センター（National Identity Service customer centres）に対して登録作業の訪問日を予約する。
④ 訪問時にIDカード発行希望者は申込書とそれに関連した証明書を持参し、指紋と顔写真、サインをNIRに登録する。
⑤ 10日前後で安全な配達方法によりIDカードが申請者に届けられる。

国民ID登録簿（National Identity Register）の登録対象はイギリス内に居住する16歳以上であった（IDカード法2条）で規定している。IDカードやその他の身元証明書類（パスポート、運転免許証等）の申請者に対し、国民ID登録簿への登録を義務付けていた[49]。登録された個人にはユニークな番号である国民ID登録番号（National Identity Register Number）が付与される（IDカード法2条）。国民ID登録簿には、身元情報（氏名、性別、生年月日、出生地、身体的特徴（生体情報含む））、主な居住地の住所、その他の居住地の住所、旧住所等の情報が登録可能であった（IDカード法1条）。

(2) イギリスのIDカード法と国民ID登録簿の廃止

政権交代の影響から政府は2010年5月26日にIDカードと国民ID登録簿構築の廃止を規定したIDドキュメント法案を提出した。同法案は2010年9月15日に下院を通過し、2010年2月21日に勅許を得てIDドキュメント法（Identity Documents Act）[50]が成立した。IDドキュメント法の第1条ではIDカード法の廃止を規定している。 IDカード法が廃止にいたった理由はいくつかあげられる。

1点目として、コストが挙げられる。政府は、IDカードスキームのコストを10年間で54億ポンドとしていた[51]。しかし、London School of Economics and Political Scienceの報告書[52]によれば、IDカードの導入に低コストで106億ポンド、高コストで

[49] "英国のバイオメトリクス計画が前進へ - 議会が国民 ID カード法案を可決". Computerworld. http://www.computerworld.jp/contents/36361, (accessed 2012-02-20)
[50] "Identity Documents Act". legislation.gov.uk http://www.legislation.gov.uk/ukpga/2010/40/contents, (accessed 2012-02-20)
[51] "ID card scheme cost put at £5.4bn". BBC News. http://news.bbc.co.uk/2/hi/uk_news/politics/6033687.stm, (accessed 2012-02-20)
[52] "The Identity Project: an assessment of the UK Identity Cards Bill and its

192 億ポンドの費用がかかると試算[53]しており、IDカードのコスト面が批判された。

2 点目として、効果が挙げられる。IDカードの導入の背景にはテロ防止があった。前述の内務大臣のデビッド･ブランケットは､IDカード導入の検討をしていた 2004 年に、IDカードは身元詐称の利用防ぎテロリストや組織犯罪の取り締まりを支援するものと述べていた。しかし、人権グループのLibertyはIDカードではそれらを防ぐことはできないと､すでにIDカードスキームのあるスペインで発生した 3 月 11 日のテロ事件を例に挙げ、指摘した[54]。

3 点目として、プライバシーの懸念がある。情報コミッショナー事務局のリチャード・トーマス（Richard Thomas）は、2004 年 7 月 30 日のプレスリリースで、NIR の設置はデータ及びプライバシー保護の観点から懸念があると述べた。彼はなぜ多くの個人情報を収集し、NRIに保存される必要があるのか疑問を投げかけ、行政やその他機関が個人はどのように生活しているか包括的にみることができる可能性があることの危険性を述べた[55]。

(3) 民間IDの利用の動き（Identity Assurance Services）

IDカード法と国民ID登録簿が廃止になり、Identity Assurance Servicesの計画を発表した。内閣府大臣フランシス・モーデ（Cabinet Office minister Francis Maude）によれば、Identity Assurance Servicesの目的は、民間部門のアイデンティティ保証サービスの市場を創造し、国民が公共サービスにアクセスする際の自身のアイデンティティを証明するプロバイダーの選択を許すことであるとしている[56]。

Identity Assurance Servicesとは、銀行、スーパーマーケット、SNS、郵便局などのアイデンティティ・プロバイダーが発行するIDを用いてイギリス政府は公共部門の全てのオンラインサービスで利用できるようにするものであり、The Government

---

implications". London School of Economics and Political Science. http://www.lse.ac.uk/collections/informationSystems/pdf/projects/identityreport.pdf, (accessed 2012-02-20)

[53] "ID cards - UK's high tech scheme is high risk". London School of Economics and Political Science. http://www.lse.ac.uk/collections/informationSystems/research/researchProjects/identityProject/IDcardsUKsHighTechSchemeIsHighRisk.htm, (accessed 2012-02-20)

[54] "ID cards 'cannot stop terrorism'". BBC News. http://news.bbc.co.uk/2/hi/uk_news/politics/3655497.stm, (accessed 2012-02-20)

[55] "Information Commissioner Publishes Concerns on Identity Cards". Local Government Chronicle (LGC). http://www.lgcplus.com/information-commissioner-publishes-concerns-on-identity-cards/1231808.article, (accessed 2012-02-20)

[56] "Government outlines plans for identity assurance services". ComputerWeekly.com. http://www.computerweekly.com/news/1280095921/Government-outlines-plans-for-identity-assurance-services, (accessed 2012-02-20)

Digital Serviceのひとつのプロジェクトとして取り組まれている[57]。

3.3.2 midataという新たな試み（自己情報の利用権限の付与）

(1) midataの概要

イギリスのビジネス・イノベーション・職業技能省（BIS：Department for Business, Innovation and Skills）が2011年4月13日に消費者権限付与戦略（Consumer Empowerment Strategy）を発表した。その第1章に"midata"プロジェクトがある。（2011年4月13日の文書ではmydataと記述されたいたが、その後midataと改称した）

消費者に権限付与することで、消費者が「より良い選択・より良い取引（Better Choice Better Deals）」ができ、長期的な経済成長につながると述べている。消費者が常に「より良い選択・より良い取引」ができるのならば、消費者は安心して、消費活動ができ、経済がまわると考えられる。「より良い選択・より良い取引」をするためには、消費者のこれまでの経験をもとにした消費傾向、ニーズを分析し、その個人にとって最適なサービスや商品、料金体系の情報を利用することで実現される。これら情報は企業側にあり、それを消費者がアクセスし、コントロールし、利用することができれば良く、時には、分析を得意とするサードパーティー渡すこともできれば良いと考えられる。

すなわち、midataとは、消費者が企業の保持している自身のパーソナル・データにアクセスし、そして利用できるようにするプロジェクトである[58]。

(2) midataによるアクセスと利用

midataとは、消費者が企業の保持している自身のパーソナル・データにアクセスし、そして利用できるようにするプロジェクトであるが、そのアクセスや利用については現状としてイギリス国内ではどのようになっているだろうか。

midataプロジェクトの資料では、個人が企業の保持する自分情報へのアクセスの現状として法律や制度としては認められているが実効性はあまりないと述べている。情報公開の問題は、今まで政府によって保持されているデータセットに焦点が当てられてきた（情報権（right to data））。情報公開に関する問題の次のステージは企業が持つ個人に関するデータであるという。データ保護規制（Data Protection legislation）の下では、消費者は「国民アクセス権（subject access rights）」を介して）企業が持つ

---

[57] "Government Digital Service". Cabinet Office. http://digital.cabinetoffice.gov.uk/about/, (accessed 2012-02-20)

[58] midataプロジェクトの詳細については、本報告書の5.1に

自身についてのパーソナル・データへアクセスを要求する法的権利を有している。しかしながら、最近の調査によれば、回答者の半数以上がその権利については知らず、その権利を実行した消費者はごく少数に限られている。また、企業努力としてパーソナル・データを個人にも見られるようにしていることもあるが、通常はリアルタイムでデータにアクセスすることはできず、電子形式でデータにアクセスする法的権利があるわけでもない。

企業が保持する個人の情報の利用の現状として、アクセスして閲覧することはできるが、本人がダウンロードして利用したり、誰かに（分析など）利用させることは出来ていない。銀行、電話通信、オンライン小売議業者の部門では消費者が取引履歴を見られるのは次第に一般的になってきている。大抵は画面上で見られるだけであり、共通形式でのダウンロードなどは利用できない。

(3) midataの今後の動き

個人の、事業者の保持する自分の情報に対するアクセスと利用の面を整えるため、、金融、通信、小売、オンラインおよびユーティリティ（電気・ガス・水道）部門のトップ企業が関与している。オープンで再利用可能な形式の制定や、自主協定や自主規制の開発を進めている。

プライバシー、セキュリティ、法律の面については、インターネットセキュリティ提供会社、情報コミッショナー事務局、消費者団体が関与している。プライバシーの保護に関して、プロジェクト着手時から「プライバシー・バイ・デザイン」のアプローチを用いている。リスク管理やプライバシー管理のツールキットを開発している。信頼形成に関しては、企業は正しく個人を認識し、消費者はきちんと個人情報を保護していると認識できる信頼関係（監査体制の実施と思われる）を作るような取り組みを行っている。制度やシステムによる保証に関しては、法律の修正、制定、新たなガイドラインの策定を検討している。

政府の役割としては、ビジョンの設定、消費者・企業・解説者間の利益創造の支援、効果的で安全な手段による市場作動支援を行うにとどめ、政府はデータを取り扱ったり、処理したり、閲覧することはない。

3.4 欧州委員会

3.4.1 EUデータ保護に関する包括的な改革案

欧州委員会は、2012 年 1 月 25 日、オンラインでのプライバシーの権利を強化し、欧州のデジタル経済を後押しする EU の 1995 年のデータ保護指令（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（Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data））の包括的な改正へ向けた EU 個人データ保護規則案（個人データの取扱い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規則（一般的データ保護規則）の提案：Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)）を提案した。

(1) 提案の背景

提案の背景には、1995 年の EU データ保護指令が現在の社会に適合していないことがあげられる。近時の技術進歩およびグローバル化の進展は目覚ましいものがあり、個人データの収集、アクセス、利用の方法は、1995 年当時とは大きく異なっているため、現行の EU データ保護指令では個人データ保護に対して十分に対応できていない状況が生まれている。また、27 ある EU 加盟国は、1995 年の EU データ保護指令について、各国それぞれで実装した結果、国によって執行が乖離してしまっている状況がある。

(2) 提案の利益

欧州委員会は EU 個人データ保護規則案が制定されれば次のようは利益をもたらすとしている。まず、EU 加盟国全体に適応される単一の規則があれば、各国で異なっている個人データ保護執行の分裂状況が解消され、個人データ保護に対する管理の負担が軽減され、年間、23 億ユーロのビジネス上の節約につながるとしている。そして、消費者のオンラインサービスに対する信頼が強化されることで、オンラインサービスの利用が活発となり、ヨーロッパ全体の経済成長、雇用、技術革新につながるとしている。

(3) 提案の目標

欧州委員会が提案した EU 個人データ保護規則案の目標は、将来のプライバシー権を保障するために、1995 年のデータ保護指令に定められている原則をアップデートし、近代化させることである。

(4) 提案の内容

提案には二つの法的提案が含まれる。ひとつは規則である。個人データ保護のための一般的な EU フレームワークを設置するものである。もうひとつは指令である。司法活動と犯罪行為の防止、発見、調査、起訴を目的に処理される個人データの保護を実現するものである。

(5) 提案の特徴点

提案の特徴点は以下のとおりである。

- EU 全体に渡り効力のある規則（EU 個人データ保護規則）を設置する。
- 不要な管理要件（例えば企業届出要件（notification requirements for companies））を削除した。手続きの簡素化の一方で、企業が処理する個人データに対して義務と責任を増加させるようにしている。たとえば、企業や組織は、深刻なデータ侵害（data breaches）があればできるだけ早く（24 時間以内に）国家監督機関に通知しなければならないということにした。
- 企業は主たる場所の唯一の国家データ保護機関（single national data protection authority）とだけ連絡を取れば良く、同様に、個人も EU 圏外に設置された企業によってデータが処理されていたとしても、その個人の国のデータ保護機関に問い合わせをすることで様々な対応ができるようにした。
- 個人は自分のデータへのアクセスが容易になり、あるサービス・プロバイダーから別のサービス・プロバイダーへと個人データの転送ができるように「データ･ポータビリティの権利」を認めた。
- 「忘れてもらう権利」を認めた。これは個人データを保持するための正当な根拠が存在しない場合、個人がそのデータを削除することができるようにするものである。個人がデータ保護のリスクを管理するのに役立つとしている。
- EU 圏内の人々にサービスを提供し、そして EU の市場で活動する企業によって個人データが国外で処理（handled abroad）される場合には EU 個人データ保護規則を適用しなければならないとした。
- 各国のデータ保護機関は、EU 個人データ保護規則が自国にて実行されるようにその権限を強化されるようにした。

- データ保護機関は EU 個人データ保護規則に違反した企業に罰金を科す権限が与えられる。罰金は最大 100 万ユーロもしくは企業の年間国際的売上高の 2%を上限としている。
- 新しい指令は、一般的な保護原則と犯罪事件での警察および司法協力（police and judicial cooperation）のルールを採用した。ルールは、データの国内及びクロスボーダーの転送に適用される。

3.4.2 EUデータ保護規則

EU データ保護規則案の具体的な条文内容については仮日本語訳を参考資料（5.2, p. 63）にて記載しているので参照いただきたい。

3.5 OECD

3.5.1 自然人のデジタル・アイデンティティ・マネジメント

情報セキュリティとプライバシーに関する OECD 作業部会（WPISP： the OECD Working Party on Information Security and Privacy）は、「自然人のデジタル・アイデンティティ・マネジメント：インターネット経済における革新と信頼の付与 － 政府ポリシー立案者のための指針（Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers)」を発表した。

この指針は、情報システム及び情報ネットワークのセキュリティに関する活動とプライバシー保護に関する活動の接点になる主要政策問題について、4 年にわたって行われた分析作業の集大成として位置づけられ、各国政府に対してデジタル・アイデンティティ・マネジメントに対する国家戦略の策定に向けた政策指針を提供している。

指針は大きく 2 部で構成されている。第 1 部ではデジタル・アイデンティティ・マネジメントの重要性と中核に触れ、なぜ必要なのか、現状の何が問題なのか、解決に向けた政府の役割は何か、紹介されている。第 2 部では、デジタル・アイデンティティ・マネジメントに対する国家戦略の策定に向けた政策指針がなされている。

なお、詳細は参考資料（5.2, p.63, 参照）を参照いただきたい。

3.5.2 インターネット経済のコアはデジタル・アイデンティティ・マネジメント

OECD では、デジタル・アイデンティティ・マネジメントはインターネット経済のコアであるという。

インターネットが出現したばかりの 1990 年代を振り返ると、ハイパーリンクをクリックするだけで誰でもインターネットに接続して情報を入手できるということは革命的な出来事であった。しかし、それから数年の間に新たな革命が起こった。その革命とは単にインターネットは情報が入手できるというだけでなく、個人の認証によって双方向関係を確立し、様々なサービスを提供することが可能となったことである。

インターネットが情報の公開から個人向けサービスの相互作用プラットフォームに進化したことにより、電子商取引、電子政府の他、電子医療システムや電子学習システムからソーシャル・ネットワークなど、豊富かつ多数のオンライン相互作用が可能になった。個人の認証が可能になり、相互作用プラットフォームが確立したことは、その後の 10 年以上にわたる技術革新、インターネットの普及、ユビキタス性及び日常生活における必須性、経済社会の変化及びインターネット経済の構築を実現した大きな進歩の 1 つである。インターネット経済においては、その参加者たる個人のデジタル・アイデンティティのマネジ

メントなしには、インターネット経済は成り立たないとしている。

3.5.3 政府のための政府ポリシーの指針

OECD が発表した「自然人のデジタル・アイデンティティ・マネジメント：インターネット経済における革新と信頼の付与　政府ポリシー立案者のための指針」では、政府ポリシー立案者のための指針を紹介している。

(1) デジタル・アイデンティティ・マネジメントの明確な国家戦略を採用すべきである

デジタル・アイデンティティ・マネジメントの明確な国家戦略は、オフラインの経済的・社会的サービスのデジタル世界への移行、革新的なオンラインサービスの創造、インターネット経済の継続的発展には必須であり、企業、市民、そして政府を含め、社会全体としての利益を達成すべきである。

(2) インターネット経済の潜在的な長期利益を視野に入れるべきである

政府は、例えば高価値な公共または民間サービスのオンラインへの移行などの長期的な目標の必要性と達成の複雑さを理解すべきである。政府は長期目標と長期目標を達成する手段である中期・短期的目標を区別するべきであり、長期的目標の達成を妨げる短期間のソリューションを避けるべきである。

(3) 既存のオフライン・アイデンティティ・マネジメントの実装から始めるべきである

政府のアイデンティティ・マネジメント政策と実践は、その国の歴史、文化、政府の形態に深く根付いている。デジタル・アイデンティティ・マネジメントに関する政府戦略は、既にあるその国のアイデンティティ・マネジメント・システムの上に、必要に応じた進化を導入しながら、考慮すべきである。現在のオフラインの ID が信頼できないものならば、オンラインでも信頼はできない。オフラインのアイデンティティ・マネジメント政策や実践が確立されていない国ではデジタル世界への移行はより複雑になる。現在のオフライン・アイデンティティ・マネジメントの政策と実装が効果的でないならば、オンライン移行に先だってそれらは改良されるべきであり、かつアイデンティティ・データ収集の最小化を促進させプライバシー保護を改善するオンラインへの移行をうまく利用するべきである。

(4) 電子政府の活動は国家戦略と足並みをそろえなければならない

デジタル・アイデンティティ・マネジメントは政府の中では分野横断的なものであ

り、国家戦略を最大限効果的にするためには、電子政府の活動やサービスの特異性にかかわらず、アイデンティティ・マネジメントの政策と実装が政府全域で調整されるべきである。

(5) バランスの取れたデジタル・クレデンシャル政策は常に求められるなければならない

国家戦略は、個人が公共や民間サービスにわたり利用するデジタル・クレデンシャルの数の制限することや削減することを目標とすべきである。全世界的にユニークなクレデンシャル（このようなクレデンシャルはプライバシーの観点からセンシティブではある）の生成とその他のクレデンシャルの増加の間でバランス点を見つけるべきである。クレデンシャルの数の削減はプライバシー保護を犠牲にすべきではなく、プライバシーに優しい技術のために行われるべきである。

(6) セキュリティとプライバシーの両方を保証すべきである

保証レベルは取引のリスクレベル評価に基づくべきである。デジタル・アイデンティティ・マネジメントの実装は法律上のプライバシー保護要件に尊重すべきであり、デジタル・アイデンティティ・マネジメント・システムの発展と実施は着手の段階からデータセキュリティを含めてプライバシー保護をつめるべきである。プライバシーとセキュリティの両方を支援するためのテクノロジーの潜在的可能性を活かしつつ、適切なシュードニムの活用を含めて、可能な限り、革新的な技術的保護基準はプライバシー保護要求を強化しなければならない。

(7) クロスボーダーなデジタル・アイデンティティ・マネジメントを進めるべきである

電子行政、e コマース、その他国境を越えたデジタルサービスの高価値を促進させるデジタル・アイデンティティ・マネジメントの可能性は様々な障害によって妨げられる。政府や他の利害関係者はこれら障害を削減または最小化させるように働かなければならない。政府や利害関係者は、例えば、地域的・国際的な技術基準の活用を通して、国家のデジタル・アイデンティティ・マネジメントの相互認証をより発展させたり、相互運用の環境を創出したりするために、協力すべきである。

4　個人情報の安心安全な管理に向けた社会制度・基盤の今後

個人情報の安心安全な管理に向けた社会制度・基盤について、これまで第 2 章で論点を整理し、第 3 章でそれに関わる国際動向を見てきた。第 4 章では、これらを踏まえて、将来の個人情報の安心安全な管理に向けた社会制度・基盤について考察する。

4.1　個人情報の安心安全な管理のための包括的戦略の必要性

将来の個人情報の安心安全な管理に向けた社会制度・基盤を整えるためには個人情報の安心安全な管理のための包括的戦略が必要性であると考えられる。

個人情報について保護と利用の両立がなされる社会というのは、一個人だけで、一企業だけで達成できるものではない。あらゆる関係者が個人情報に携わることから、その関係者間で協力して達成すべき社会というのを明確にし、その社会を実現させるための戦略が必要となる。

この点について、OECD の指針においても、インターネット経済の革新と信頼のためにはプライバシー保護の観点も含めた明確なアイデンティティ戦略を、まずは策定するように勧めている。この明確な戦略というのは、企業、市民、そして政府を含め、社会全体としての利益を達成する道筋になるものであり、オフラインの経済的・社会的サービスのデジタル世界への移行、革新的なオンラインサービスの創造、インターネット経済の継続的発展には必須であるとも述べている。アメリカでは、まさにこのようなことを実践しており、NSTIC を打ち出し、OITF の活動を行っている。我が国においては、現在、保護と利用の両面から、個人情報、プライバシー、アイデンティティ・マネジメントについて、それらすべてを包含した戦略はなく、政府、企業、消費者が参加するオープンな検討の場もない状況にある。

まずは、個人情報の安心安全な管理に向けた社会制度・基盤の統一的な戦略策定とその検討の場が必要になるであろう。

4.2　適切な本人確認・本人認証を行える機能

将来の個人情報の安心安全な管理に向けた社会制度・基盤に必要なものとして、適切な本人確認・本人認証を行えることがあげられる。

4.2.1　本人認証を行うサービス

アメリカ、イギリス、OECD で共通に言われていることは、本人認証作業や ID・パスワード（クレデンシャル）所有の過多を減らすべきということである。個人にとって度重なる本人認証作業は煩わしいもので、かつ個人はクレデンシャルを管理しきれない状態にある。本人認証作業の重複は個人のオンラインサービスの利用を妨げ、経済的な発展を遅ら

せる要因と OECD は見ており、クレデンシャルの管理の限界はセキュリティを下げる要因にもつながるとしている。本人認証作業とクレデンシャルを減らすためには、個人と事業者という、1 対多の関係の間に入り、本人認証を行うサービスが必要と考えられる。

このサービスの機能として、アメリカでは民間のアイデンティティ・プロバイダーを用いた公共サービスの連携を OITF で目指している。イギリスもアイデンティティ・プロバイダーの活用を考えている。ドイツは、政府が身元を保証する主体となり、本人認証の方法として eID-Funktion を搭載した新身分証明書を発行している。

4.2.2 高い保証レベルの本人確認

これからの情報社会での本人確認を考えた場合、現在の、低い保証レベルの本人確認だけでなく、中・高程度の保証レベルの本人確認が必要になってくることがある。

OECD では、経済的価値の高いサービスをインターネットで本格化させるためには、高い保証レベルの本人確認がインターネットで可能にすることは必須であるとしている。そのため、信頼性が担保された高価値な経済的・社会的なオンライン取引を促進させるための高い保証レベルの本人確認をどう提供するかが課題となるが、ドイツでは、政府が発行した新身分証明書をオンラインでも利用できるようにしている。アメリカやイギリスは、政府が身分証明のツールを用意するのではなく、民間のアイデンティティ・プロバイダーをレベル分けし、高い保証レベルに対応したプロバイダーを認定することで、この本人確認の課題を解決しようとしている。

4.3 必要以上に自分の情報を明かさずにサービスを受けられる機能

将来の個人情報の安心安全な管理に向けた社会制度・基盤では、名寄せや個人情報の漏えいの被害を軽減させるために、必要以上に自分の情報を明かさずにサービスを受けられるようにする必要があると考えられる。

4.3.1 シュードニムの利用

個人と事業者との間では、自分の情報が広く集めることができるような横断利用可能な識別子の無制限な使用を許すのではなく、シュードニムの効果的な利用を可能にすべきである。

この識別子の点において、OECD の指針でも、システムの発展と実施は着手の段階からプライバシー保護に努めるべきであり、そのために技術的なプライバシー保護メカニズム、例えば、適切なシュードニムの利用等によって、可能な限り、強化されなければならないとしている。アメリカの NSTIC においても 4 つのガイディング・プリンシプルのひとつとして、プライバシーを強化し、自発的な参加が可能であることを挙げており、シュードニム（PPID）の利用を必須としている。ドイツにおいても、新身分証明書の機能としてシュードニムを利用可能にしている。

4.3.2 個人情報を最少化させるサービス

個人と事業者、1 対多のような関係において、個人は様々な事業者に対して情報を渡すことになる。個人に関わる情報を渡せば渡すだけプライバシーの侵害や漏えい等のリスクが高くなる。できるだけ個人情報を提供しないように最少化させることは、アメリカ、ドイツ、OECD で共通の考え方である。

情報提供を最少化させるには、事業者に不必要な情報を求めないように制限をかけることが考えられる。他にも個人と事業者の間の仲介者を置くことが考えられる。例えば、住所を教えたくないという人のための配送代行サービス、クレジットカード番号を教えたくないという人のための決済代行サービスといったものである。しかしながら、名前、住所、生年月日、電話番号、メールアドレスといった、個人を特定する基礎的な情報すべてを含めた個人情報を最少化させる仲介サービスというものはない。

必要以上に自分の情報を明かさないために、シュードニムの活用やエスクローサービスを担う存在があると良いと考えられる。その主体は 4.2 で述べた適切な本人確認・本人認証を行う主体と同一であると効果的であると考えられる。

4.4 自分の情報がコントロールできるような機能

将来の個人情報の安心安全な管理に向けた社会制度・基盤には、自分の情報がコントロールできるような機能が必要である。

4.4.1 データ・ポータビリティの担保

EU データ保護規則の改正案では、データ･ポータビリティの権利について述べている。これからの社会で大きな問題になると考えられるのが「ロック・イン」である。あるサービスを利用し始めると、それから人々を逃れさせなくするという問題である。この傾向はますます強くなることが予想される。情報が個人にとって重要な意味を持ち始めている現在、自分のデータへのアクセスが容易であることや、そのデータを自分で使えるようにすること、そしてあるサービス・プロバイダーから別のサービス・プロバイダーへとデータの移転ができるようにすることは必須である。イギリスでも同様にデータ・ポータビリティについて重要視しており、midata プロジェクトにおいて、データの移転やデータの包括的利用および変更についての方法論を検討している。

データ・ポータビリティを担保するには、そのためのルールと、ルールに従って運用されていることを監視する者が必要と考えられる。

4.4.2 忘れてもらう機能

EU データ保護規則の改正案では、「忘れてもらう権利」につい規定している。個人デー

タを保持するための正当な根拠が存在しない場合、人々がそのデータを削除することができるようにする権利である。プライバシーの観点から、個人がデータ保護のリスクを管理するのに役立つものである。

しかしながら、「忘れてもらう」にしても、個人自身がどこに何を教えたかわからないという状況では、忘れてもらう相手を特定できず「忘れてもらう」ことを「権利」として構成する意味は希薄になる。そのためには自分の情報を、いつ、誰に、どの情報を、どのような条件で提供したかがわかり、これらの機能を本人に代わって行う主体が必要と考えられる。

4.4.3 情報コントロールのサポート

インターネットでのサービスを利用する機会が多くなり、利用する情報量が膨大になると、前述の 4.4.1 及び 4.4.2 で触れた通り、個人は自分に関わる情報を把握しきれなかったり、コントロールするのは難しくなる。この自分の情報を把握できないことやコントロールできないことの弊害は、引っ越しをしたり、携帯電話番号の変更、メールアドレスの変更、クレジットカードの変更、口座の乗り換え等に現れてくる。どのサービスに、どのメールアドレスを教えたのか、あのサービスは、前の住所のままなのか、個人が確認するためにはそのサービスに問い合わせをしなければならない。仮にサービスにどういった情報が登録されているかわかっていたとしても、一人平均約 20 サイト利用している現状（図 2 3, p. 9, 参照）では、自分の状況の変化に応じてそれらすべての登録内容を適宜変更することは労力のかかる作業となる。

情報をコントロールや、データ・ポータビリティおよび忘れてもらう機能を実現させるための個人の情報コントロールをサポートする主体が必要と考えられる。その主体が、4.2 で述べた適切な本人確認・本人認証を行う主体、4.3 の必要以上に自分の情報を明かさないため機能を提供する主体と同一であってよいかについては検討する意味があると思われる。

4.5 社会制度・基盤の信頼性の担保

適切な本人認証ができ、必要以上に自分の情報を明かさずにサービスを受けられ、自分の情報がコントロールできるようにするための仕組みが社会制度のような形で提供されるならば、最終的にそれらの信頼性や実効性を担保する必要がある。そのためには制度のポリシー策定、信頼形成のための監査、紛争が生じたときの手続や処理といったことを行う、公平性、透明性のある第三者の存在が必要である。

4.6 個人情報の安心安全な管理に向けた社会制度・基盤の実現

これまで述べてきた、適切な本人認証を行える機能、必要以上に自分の情報を明かさずにサービスを受けられる機能、自分の情報がコントロールできるような機能を実現するた

めには戦略的な取り組みをしなければならない。社会制度・基盤に関係する者の役割の明確化、経費的な面を含めたビジネスモデル、ルール違反をとがめる法制度等の裏打ち、人材育成など、多岐にわたる検討を行うことが、実現のためには必要であると考えられる。

5　参考資料

5.1 Better Choices: Better Deals（仮日本語訳）

第 1 章：情報の力

第 1 章　主要な事実と数字

もし消費者ができるだけ効果的に価格比較サイトを使用する場合、彼らは年間、1 億 5 千万～2 億 4 千万ポンドも得をする。[15]

価格比較サイトを使用する人の 13%のみが最低価格の店から購入する。[16]

消費者がいつも正確な情報を持っていないというのも理由の一つだが、予測するのが難しいというのもある。[17]

最近の EU の調査では、英国の消費者は、価格比較、取引条件の精読、消費者情報への関心の点において、欧州で最も低い値を示すことがわかっている。[18]

企業はこれを上手く利用することができる。例えば、米国の研究では、延滞料がビデオレンタル店の収益の最大 20%を占めていることがわかった。[19]

あまりにも多くの選択肢と情報は抗し難いものになるので、個々人は多くの情報を必要とはしていないだろうという証拠もある。[20]

私たちは"情報時代"に生きている。情報は自由に交換され、コンピューター、携帯電話やインターネットが誕生する前では不可能であったり、難しかったりした知識に個人はアクセスできる。

情報は、5 年、10 年前に比べ、はるかに容易に利用でき、デジタルデータは自動収集メソッドの向上や、ストレージの大容量化によって、急激な増加をもたらしている。最近のスマートフォンの出現はアプリケーションとトラッキング技術で、企業や個人が新しく、かつエキサイティングするような方法でデータを利用する、新しい時代を導いている。

15　Office of Fair Trading (2007) Internet Shopping – an OFT market study, OFT921. London: Office of Fair Trading
16　Baye M, Morgan J and Scholten P (2004) Price Dispersion in the Small and in the Large: Evidence from an Internet Price Comparison Site. The Journal of Industrial Economics 52(4) 463-496
17　Della Vigna S and Malmendier U (2006) Paying Not to Go to the Gym. American Economic Review 96: 694-719
18　European Commission (2011) Consumer Empowerment: Eurobarometer 342. Brussels: European Commission
19　Ayres I and Nalebuff B (2003) In Praise of Honest Pricing. MIT Sloan Management Review 45(1): 24-28
20　Schwartz B (2004) The Tyranny of Choice. Scientific American 290: 70-76

現代の情報処理技術は、例えば、ポイントカードやインターネットの購買履歴を通して、企業が消費者の購買決定と個々人の特性についてのデータを積極的に収集できるようにしている。これはより洗練された'顧客管理'を可能にし、企業が消費者の要求を切り分けたり、適合させたりできるようにさせる。例えば、特に顧客が興味を持つかもしれない商品の提案、その商品に関連した商品の安売り、そして、企業にとって有益な（しばしば狙われやすく不利な立場にいる）顧客の識別可能性に役立つ。[21]

これらの試みは、企業が顧客に対して、商品やサービスの質や価格、そして選択肢という有益な情報を与え、それらは価格を引き下げるので歓迎されるべきものである。[22] 多くの場合、個人の購入履歴のデータの成長は、"もしあなたがこの映画、本、ホテルを好んでいるとしたら、あなたは X も好きかも知れない……"と、企業が提供すサービスの向上を有効にしている。しかしながら、このような知識は、消費者自身が知る以上にその消費者の好みを企業が知るというような、経済学者の言う'情報の非対称性'を造りだす。[23] 例えば、クレジットカード会社は、分割での支払が完了できるかという可能性について消費者自身よりも知っているかもしれない。場合によっては、企業はこの情報の優位性を、消費者が過大評価する値引価格や料金表を作ために使うかもしれない。[24]

詳細情報へアクセスが必ず役立つというわけではない。ある研究者では規制によって要求された情報の多くはターゲット層に到達しないと示している。[25] あまりにも多くの情報があることで、ある意味、消費者を思いとどまらせるようなことを引き起こすからである。あまりにも多い情報は'選択肢過多'を引き起こし、選択肢過多は消費者の決定を難しくさせる。それゆえ情報は（'認知コスト'を減らすために）理解しやすい形式で、かつ、（'実行コスト'を減らすために）消費者が決定しやすいような方法で提供されるべきである。[26] 近年、私たちが見てきているように、携帯電話の料金表や保険の掛け金のような複雑な情報の分析をしたり、消費者がよりよい取引に切り替える手助けをするような役割をする仲介人やオンラインプラットフォームが出現している。

詳細情報へアクセスが必ず役立つというわけではない。ある研究者では規制によって要求された情報の多くはターゲット層に到達しないと示している。あまりにも多くの情報があることで、ある意味、消費者を思いとどまらせるようなことを引き起こすからである。あまりにも多い情報は'選択肢過多'を引き起こし、選択肢過多は消費者の決定を難しくさせる。それゆえ情報は（'認知コスト'を減らすために）理解しやすい形式で、かつ、（'実行コスト'を減らすために）消費者が決定しやすいような方法で提供されるべきである。近年、私たちが見てきているように、携帯電話の料金表や保険の掛け金のような複雑な情報の分析をしたり、消費者がよりよい取引に切り替える手助けをするような役割をする仲介人やオンラインプラットフォームが出現している。

この章では、消費者権限付与の情報政策に関してふたつの政府優先事項を提示し、同時に、前述の優先事項を実施するための提言をする。

１．パーソナル・データへのアクセス：消費者が企業によって保持されている消費者のパーソナル・データにアクセスし、そして利用できるようにさせる：'mydata'

２．情報の価値強化：消費者が使用している商品やサービスについてよりリッチで、より適切な情報を消費者が得られることを保証する新たな提案

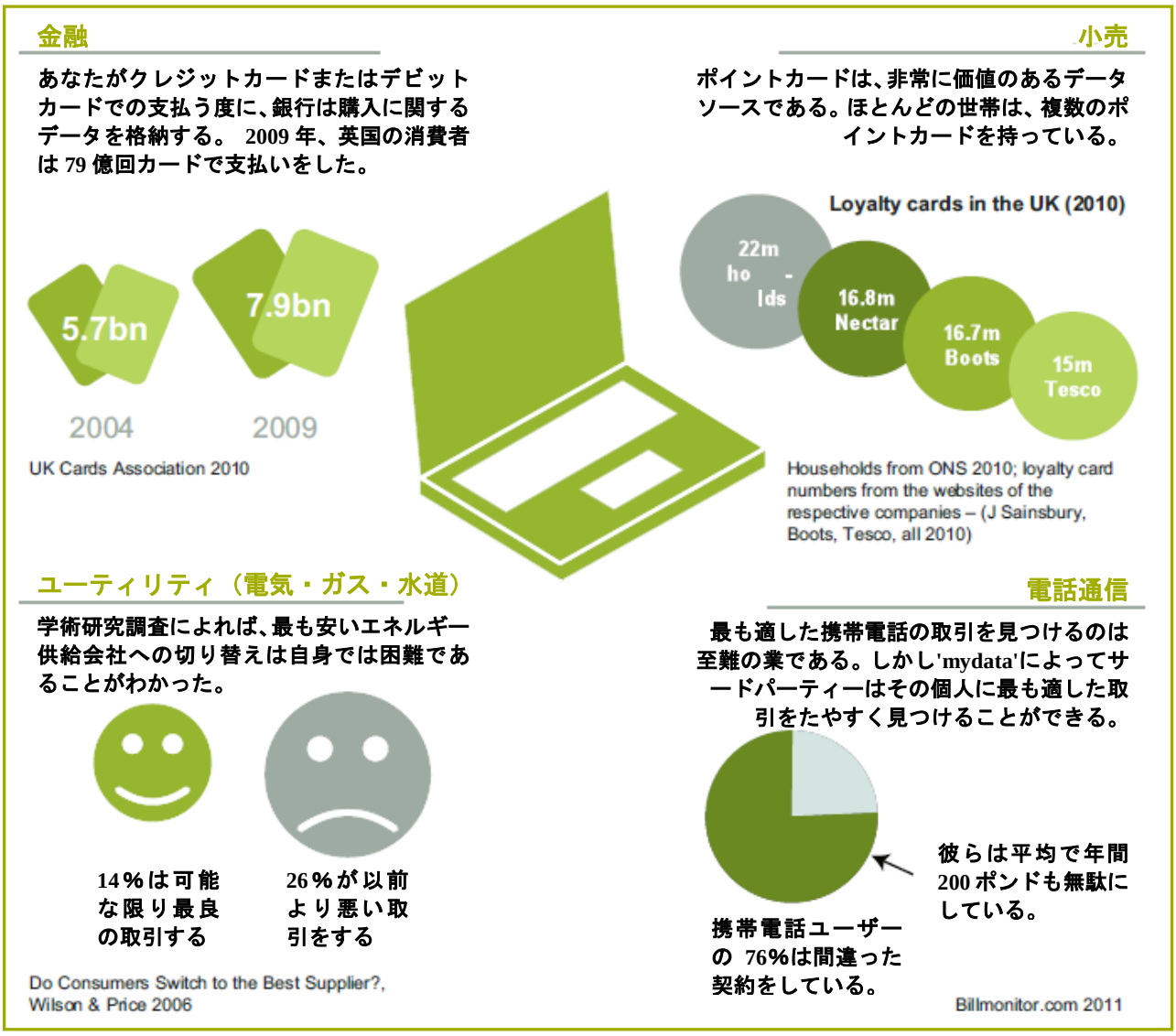
21 Ayres I (2007) Supercrunchers: Why thinking-by-numbers is the new way to be smart. New York: Random House
22 Kamenica E, Mullainathan S and Thaler RH (2011) Helping consumers know themselves. Available at SSRN: http://ssrn.com/abstract=1742505
23 Ayres I (2007) Supercrunchers:Why thinking-by-numbers is the new way to be smart. New York: Random House
24 Kamenica E, Mullainathan S and Thaler RH (2011) Helping consumers know themselves. Available at SSRN: http://ssrn.com/abstract=1742505
25 Better Regulation Executive and National Consumer Council (2007) Warning:Too much information can harm. London: BIS
26 Schwartz B (2004) The Tyranny of Choice. Scientific American 290: 70-76

消費者が企業によって保持されている消費者のパーソナル・データにアクセスし、そして利用できるようにさせる：'mydata'

政府の透明性や情報公開の問題は、今まで政府によって保持されているデータセットに焦点が当てられてきた。つまり、具体的には、政府によって保持されているデータセットを大部分の国民が要求し、使えるようにさせる'情報権（right to data）'がそうである。[27] 情報公開に関する問題の次のステージは企業が持つ個人に関するデータに焦点が当てられ、同時に消費者が様々な方法で自身のパーソナル・データにアクセスし、コントロールし、利用できるようにすることであろう。消費者が企業に保持されているデータにアクセスすることが容易で簡単になれば、仲介業者のような者は、消費者に購入選択時の理解を深めさせるため、異なったソースからのデータを結合したり組み合わせたりすることが可能になるだろう。競争を促したり、情報を伴う問題を削減したり、検索したり、コストを切り替えたりすることで、消費者の価値や選択時の改善に結びつくだろう。それゆえ、このような活動は、消費者の過去のサービス利用の正確な情報に基づき、消費者が決定したり、売り手による価格競争がなされる世界に向けた重要な足がかりとして機能するだろう。

我々はこの野心的なプログラムを'mydata'と呼んでいる。

パーソナル・データ



27 HM Government (2010) The Coalition: Our programme for government

大きな経済的価値は、主要小売業者、銀行、電話会社、ユーティリティ、インターネットの仲介や他の企業が保有する個人に関するデータの中に閉じ込められている。[28] データ保護規制（Data Protection legislation）の下では、消費者は（'国民アクセス権（subject access rights）'を介して）企業が持つ自身についてのパーソナル・データへアクセスを要求する法的権利を有している。しかしながら、最近の調査によれば、回答者の半数以上がその権利については知らず、その権利を実行した消費者はごく少数に限られている。[29] 実際のところ、（最長で 40 日間以内という制限があるので）通常はリアルタイムでデータにアクセスすることはできず、また電子形式でデータにアクセスする法的権利があるわけでもない。

蓄えられたパーソナル・データの量というのは、消費者と共有されているかに関わらず、セクター間やセクター内部で、大きな格差がある。例えば、銀行、電話通信、オンライン小売議業者の部門では、消費者が取引履歴を見られるようにすることは次第に一般的になっている。しかしながら、画面上で見られるだけあり、一般的な形式でダウンロードできるわけではない。もしダウンロードが可能であるならば、仲介業者やサードパーティーが消費者に対して、例えば、これまでの個人の利用から最も適した料金体系や消費傾向といった明確な情報を消費者に与えるなど､容易に再利用できるようになるだろう。（現在ダウンロードできる形式ではないので）その結果として、これら分野の仲介業者やサードパーティーは、しばしば消費者からのログインを通じて消費者による詳細情報の提供に頼ることや、データを'かき集める（scrape）'などの、代替方法を使わざるを得ない。

'mydata'：何であり、何でないのか。

'mydata'とは、消費者のパーソナル・データを消費者自身がコントロール、アクセスさせるために消費者団体とリーディングカンパニーと協力して実施するプログラムの呼称である。mydate は、ポータブルかつ安全な方法で消費者が自身の取引情報へアクセスできるようにさせ､その情報を扱うことのできるアプリケーションの増加を上手く利用し、消費者がより良い取引を見つけたり、消費傾向のある商品を教えたりすることが目的である。

これは消費者がパーソナル・データを共有したり、アクセスしたりしなければならないという意味ではない。すべての人がこれらアプリケーションを使いたいのではないので、使いたい人のために、アプリケーションはデータを誰とどのように共有するかを明確にすることができるようにすべきである。これは政府がデータを見たり共有したりすることを意味するのではない。このプロジェクトを可能にさせるエキサイティングなアプリケーションが発展するかは、データを保持し処理する大企業だけでなく新規の小さなハイテク企業含めた市場次第である。私たちは新しいアプリケーションと同じだけ期待するかもしれないが、政府が一連のプロセスを実施するわけではない。もちろん、新しいツールや技術はプライバシーリスクを取り除く必要があるだろう。政府の役割は、ビジョンの設定、消費者・企業・解説者（commentators）間の利益創造の支援、効果的で安全な手段による市場作動（market operate）支援、である。

情報コミッショナー事務局は、一般国民ために情報権の保護を維持し、政府の情報公開や個人のデータ機密性を促進させる英国の独立機関である。情報コミッショナーは次のように述べている：

より大きな公開性を促進させ、国民がいま以上にパーソナル・データをコントロールするためのこの構想を私は強く支持します。'mydata'は、データ保護法の要件と互換性があります。消費者権限付与戦略は、法令遵守と国民の信頼が維持されるのか、プライバシーとセキュリティの次元は適切な管理下に置かれる必要がある。プロジェクトは'プライバシー・バイ・デザイン'のアプローチを用いて着手から注意深さを求めている。情報コミッショナー事務局は消費者権限付与を得るための'mydata'作業部会を喜んで支援するだろう。

28 Ayres I (2007) Supercrunchers: Why thinking-by-numbers is the new way to be smart. New York: Random House
29 Which? (2011) Online Omnibus Survey (1,336 adults aged 16+)

消費者は当然プライバシーとセキュリティの問題が心配になる。実際に我々は、データアクセス権とプライバシーリスクだけでなく、それらリスクの管理するツールやシステムの市場の両方を強く意識する重要な政府政策目標を'mydata'に掲げることを望んでいる。

'mydata'とそれが実際に意味すること

朝	昼	晩
07:00 シャワーを浴びる "どのくらいのエネルギーを私は一日で利用するのだろうか？"	**12:00 昼食** "私は普段昼食にいくらかけているのか？"	**19:00 ネットショッピング** "どのくらい日常消費を抑えることができるのだろう？"
08:15 現金自動預け払い機 "私は通常どのくらいのお金を引き出し、最後に利用してからどれくらい立っているのか？"	**14:00 携帯電話** "私にとって一番適した料金体系は？"	**19:30 ネットバンキング** "どのくらい私は一年間でクレジットカードの手数料を支払っていうのか？"
08:30 通勤 "最短ルートは何だろう？"	**18:00 スーパーマーケット** "どれくらいの頻繁で5-a-day（野菜や果物を１日５皿以上食べようとする運動）をしているのか？"	**23:00 就寝** "廊下の照明にどれだけ費用をかけているのか？"

企業はあなたの疑問に答えるためにデータを使う……

……だけでなく'mydata'はあなたにも可能性を与える。

'mydata'の導入で起こる変化には、消費者が消費パターンを理解する手段が変化するという潜在的可能性を秘めている。個人に最適化されかつ簡略化された検索は、より効果的で安い製品やサービスに切り替えるサポートする。そして、'mydata'は消費者に購入決定の際の興味深く、重要で、有益なものを押してくれるサービスといった新たな市場を開拓する。重要なことは、現在企業が保持している消費者のデータを消費者がよりコントロールするようになることである。

これは、消費者がデータを理解し、もっとも良い取引をするという難しい仕事を要求するものではない。例えば、もし携帯電話の契約を更新するならば、'mydata'は、消費者が前年支払った携帯料金の履歴を携帯電話オペレーターに要求することを許すのである。消費者は獲得した情報を信頼できるサードパーティーに渡して、過去の実際の行動に基づき、ネットワークを介して最適な料金を見つけてもらう。

消費者はクレジットカード、デビットカード、ポイントカードからのデータに近くになり、実際に商品やサービスに通常支払っている額と自由に使える収入との割合を理解することができる。例えば、レストラン、スーパーマーケット、オンラインショップでの食費の内訳を分析してより安い取引や環境に優しい代替商品を見つけることができる。新たなプライバシーテクノロジーと'ユーザー中心'のアーキテクチャーは、データに新たな意味を持たせ、プライバシーが安全な方法でサードパーティーとの共有を可能とする。

アプリケーションの市場は急速に増加している。例えば、財務管理、エネルギー消費、フィットネスや旅行に関することにおいて、('ゲーミフィケーション'と呼ばれるように）競争、比較、協調の要素を含めつつ、消費者が個人の目標を達成するアプリケーションやサービスの最近の増加がある。この働きの最も魅力的なことは、私たちが、近い将来使われるデータがエキサイティングで革新的な方法を創造することができることである。

情報の交換において信頼を形成すること、すなわち（正しく個人を識別し認識する）企業と（一貫したプロセスの中で情報がきちんと保護されていると認識する）消費者の関係は、この新しい（mydata）というプロジェクトの潜在的可能性の実現には必須である。しかしながら我々は、このプロジェクトにおいては政府の役割にデータの閲覧や処理を含めることは一切ないと強調したい。

政府の役割は、ビジョンの設定であり、消費者・企業・解説者間の利益創造の支援、効果的で安全な手段による市場作動支援、である。政府は、アクセス障壁の排除、特に科学技術に強くなく、インターネットやスマートフォンにアクセスできないような消費弱者の支援や、この先進的な発展を利用したいと望む人全てが利用できるように保証すべきである。私たちは中小企業への負荷や不利を望んではいない。私たちは関わりたいと望む者の支援を考えている。私たちは弱く狙われやすい消費者の代表や関心のある中小企業とともに、彼らのニーズに応える提案を開発するために活動する。

企業が現在保持し開放するデータの操作にかかるコストやプライバシーへの影響を考えるならば、'mydata'は一晩で簡単に出来上がるようなものではない。しかしながら我々はできるだけ早く実現するために企業と消費者団体とともに活動をしている。

冒頭で説明したように、消費者権限付与戦略は、非規制的アプローチを通してその目的を達成しようとしている。これまでに多くのパートナーからの肯定的な反応を考えると、我々は自主的アプローチが'mydata'の急速な進歩を確立するだろうと信じている。しかし、私たちのビジョンにある進展が（開放されるデータの形式となる標準化の合意の達成が失敗するように）不当に遅延するならば、または情報にアクセスしようとする消費者が深刻な問題に出くわすならば、政府は、立法を含めて適切な救済策を検討するだろう。

そのため、我々は、'mydata'を推進し、取りまとめていくため、金融、通信、小売、オンラインおよび（電気・ガス・水道）ユーティリティ部門の主な企業、インターネットのセキュリティ企業、情報コミッショナー事務局、消費者団体と政府からなる作業部会を設立した。2011 年 3 月、ダウニング街 10 番地（英国首相公邸）にて、'mydata'を生み出すために作業部会を組織する円卓会議が開催された。トップ企業、すなわち、バークレイカード、マスターカード、HSBC（香港上海銀行）、RBS（ロイヤルバンク・オブ・スコットランド）グループ、ロイズ TSB（トラスティー・セービング・バンク）、ジョンルイスパートナーシップ、グループエアロプラン（ネクター）ホームリテールグループ、セントリカ、スコティッシュ・アンド・サザン・エナジー、エヴリシングエヴリウェア（T-Mobile/Orange）そして Google は、既に作業部会に登録した。'mydata'の早期導入とパートナーになることを希望するその他の企業や組織は、BIS を経由で連絡してほしい。
（www.bis.gov.uk/better-choices）

このグループは、オープンで再利用可能な形式でのパーソナル・データの開放をするための自主協定や自主規制を開発するタスクがある。このグループはオープン、再利用可能な形式で個人データを解放するために自主規制、自主協定を開発する使命を帯びている。労働・消費・郵便事業大臣（The Minister for Employment Relations, Consumer and Postal Affairs ）が議長を務め、四半期ごとの進捗チェックと正式な年一度（2012 年 4 月）の進捗状況の見直しを行う。

グループは四半期ごとの進捗状況のチェックのために集まるが、最初はデータ開放のための形式とスケジュールについて合意するため分野ごとのサブグループを始動させる。ナイジェルシャドボルト教授（Prof. Nigel Shadbolt）が議長を務め、グループ全体の推進と協調を図る。

さらに、分野横断的な'プライバシー、セキュリティ、法律'サブグループは、保護レベルに十分な消費者のデータ移転と、信頼とセキュリティシステムを保証をするためインターネットセキュリティ提供会社とともに実施し、情報コミッショナー事務局とともに新たなガイドラインやツールキットの開発をするだろう。このグループは、法的枠組みにおいて、適切に法律を修正したり、新たに制定する必要性があるかどうかも考慮するだろう。全国市民助言局協会（Citizens Advice）、ウィッチ（Which?）やコンシューマ・フォーカス（Consumer Focus）のような、消費者団体はプライバシーグループと同じように、消費者の懸念やニーズの合致を保証するために支援や異議の申し立てなど積極的に関与するだろう。

5.2 Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers（仮日本語訳）

序文
FOREWORD

このレポートは 2011 年の OECD 加盟国におけるデジタル・アイデンティティ・マネジメントの国家戦略の比較分析の調査結果にもとづいている。このレポートは情報セキュリティとプライバシーに関する OECD 作業部会（WPISP : the OECD Working Party on Information Security and Privacy）による数年間に及ぶデジタル・アイデンティティ・マネジメントの活動の集大成である。このレポートは、OECD コンサルタントである Nick Mansfield とともに事務局（科学技術産業局 Laurent Bernat）によって作成された。

This report builds on the findings of the 2011 comparative analysis of national strategies for digital identity management in OECD countries. It represents the culmination of several years of work on digital identity management by the OECD Working Party on Information Security and Privacy (WPISP). It was prepared by the Secretariat (Laurent Bernat, of the Directorate for Science, Technology and Industry) with Nick Mansfield, consultant to the OECD.

OECD 電子行政ネットワークでの情報の恩恵を受けた本レポートは 2011 年 10 月情報・コンピューター・通信政策委員会（ICCP）によって機密解除された。

The report, which had the benefit of input from the OECD Network on E-Government, was declassified by the OECD Committee for Information, Computer and Communications Policy (ICCP) in October 2011.

自然人のデジタル・アイデンティティ・マネジメント：
インターネット経済における革新と信頼の付与
DIGITAL IDENTITY MANAGEMENT FOR NATURAL PERSONS: ENABLING INNOVATION AND TRUST IN THE INTERNET ECONOMY

政府ポリシー立案者のための指針
GUIDANCE FOR GOVERNMENT POLICY MAKERS

デジタル・アイデンティティ・マネジメントは、インターネット経済の今後の発展にとって欠かせないものである。この文書では、自然人のデジタル・アイデンティティ・マネジメント戦略を策定する妥当性を論証した上で、それに関するポリシー立案者への指針を提示する。この文書は、情報セキュリティとプライバシーに関するOECD作業部会（WPISP：the OECD Working Party on Information Security and Privacy）が、情報システム及び情報ネットワークのセキュリティに関する活動とプライバシー保護に関する活動の接点になる主要政策問題について、4 年にわたって行った分析作業の集大成である。この指針は、電子認証に関するOECD 理事会勧告（the OECD Council Recommendation on Electronic Authentication）[59] に基づいているのと同時に、インターネットの未来に関するソウル閣僚会議宣言（the Seoul Ministerial Declaration on the Future of the Internet Economy）[60]に対する回答でもある。この指針は 2002 年のOECD ガイドライン（セキュリティ文化の普及に向けた情報システム及びネットワークのセキュリティのためのガイドライン（Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security））並びに 1980 年のOECD ガイドライン（プライバシー保護及び個人データの国際データ流通に関するガイドライン（Protection of Privacy and Trans border Data Flows of Personal Data））と一致する。

Digital identity management is fundamental for the further development of the Internet Economy. This document makes a case and offers guidance to policy makers for developing strategies for the management of digital identity of natural persons. It is the culmination of four years of analytical work by the OECD Working Party on Information Security and Privacy (WPISP) on a major policy issue at the intersection of its activities on security of information systems and networks and on privacy protection. The guidance builds on the OECD Council Recommendation on Electronic Authentication and responds to the Seoul Ministerial Declaration on the Future of the Internet Economy. It is consistent with the 2002 OECD

[59] This guidance should be considered in conjunction with relevant analytical reports listed in the references and in particular the comparative analysis of national strategies for digital identity management (OECD,2011).

[60] In the Seoul Declaration, ministers declared that, to contribute to the development of the Internet economy, they “will […] strengthen confidence and security, through policies that […] ensure the protection of digital identities and personal data as well as the privacy of individuals online.” See OECD, 2008b.

Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security and the 1980 OECD Guidelines on the Protection of Privacy and Trans border Data Flows of Personal Data.

この文書は、今後のインターネット経済の発展にとって、なぜデジタル・アイデンティティ・マネジメントが不可欠であるかについて説明する。この文書は、高価値なサービスに求められる堅牢性とクレデンシャル管理の複雑さに関係する現在の取り組みの限界に対処する必要性について強調する。この文書は、公的分野と民間分野にわたる革新のための効率的なフレームワークの条件を設定する政府ポリシー立案者のための指針とともに、インターネット経済における、信頼とプライバシー、セキュリティの向上を提供する。
The document explains why digital identity management is fundamental for the further development of the Internet economy. It highlights the need to address limitations in current approaches related to the complexity of credential management and the robustness required for high value services. It provides guidance to government policy makers for setting efficient framework conditions for innovation across the public and private sectors while enhancing security, privacy and trust in the Internet Economy.

デジタル・アイデンティティティ・マネジメントは多くの観点からアプローチすることができる。例えば、デジタル・アイデンティティティ・マネジメントをうまく実施するための業務プロセス・リエンジニアリングや技術であり、それらの重要性は認知しているとは言え、この文書は、ハイレベルな公共ポリシーコンセプトに焦点を置いており、経済的かつ社会的目標が技術的実施を決めるべきでありその逆はないという見方を反映している。
Digital identity management can be approached from many perspectives. While recognising the importance, for example, of technology and of business process reengineering for successfully implementing digital identity management, this document focuses on the high level public policy concepts, reflecting the view that economic and social objectives should determine technical implementation rather than the reverse.

アイデンティティティ・マネジメントは人間、事業体、装置又はソフトウェアアプリケーションに適用することができる。この指針では、インターネットを初めとするデジタルネットワークを通じて、公共および民間部門の組織（「サービスプロバイダ」[61]）の情報システムと相互作用する自然人（「個人」）に焦点を当てる。
Identity management can be applied to human beings, business entities, devices or software applications. This guidance focuses on natural persons (“individuals”) interacting with the information systems of public and private organisations (“service providers”) through a digital network such as theInternet.

第 1 節ではインターネット経済における信頼と革新を可能にさせるものとしての公共政策の観点からデジタル・アイデンティティティ・マネジメントについて紹介する。第 2 節では、デジタル・アイデンティティティ・マネジメントに対する国家戦略の策定に向けた政策指針も提供する。

[61] The expression “service providers” relate to providers of services on the Internet and should not be confused with organisations which provide connectivity or access to the Internet.

The first section introduces digital identity management from a public policy perspective as an enabler for innovation and trust in the Internet economy. The second section includes policy guidance for the development of national strategies for digital identity management.

1. デジタル･アイデンティティ･マネジメントはインターネット経済の中心的存在である。
I. Digital identity management is at the core of the Internet economy

世界規模のウェブが出現したばかりの 1990 年代を振り返ると､ハイパーリンクをクリックするだけでだれでもインターネットに接続して情報を入手できるという事実は、革命的な出来事であった。しかし、それから数年の間に新たな革命が起こり、個人は情報及びサービスを個人に提供するためにその個人が誰であるかを考慮に入れることができ、離れたコンピュータシステムとの双方向関係を確立できるようになった。

Back in the mid 1990s, in the early days of the World Wide Web, the capacity for anybody connected to the Internet to access information, simply by clicking on hyperlinks, was revolutionary. However, within the span of a few years, another revolution took place: the possibility for individuals to establish interactions with remote computer systems which were able to take into account who they are in order to deliver information and services in a personalised manner.

ウェブがこのように媒体の公開から個人向けサービスの配信向け相互作用プラットフォームに進化したことにより、電子商取引、電子政府の他、電子医療システムや電子学習システムからソーシャル・ネットワークさらにはより広い参加型ウェブまで、豊富かつ多様な多数のオンライン相互作用が可能になった。個人が離れたコンピュータシステムとの個人的相互作用を確立し、それによる認証が可能になったことは、10 年以上にわたる技術革新においてインターネットの普及、ユビキタス性及び日常生活における必須性、経済社会の変化及びインターネット経済の構築を実現した大きな進歩の 1 つである[62]。

This evolution of the Web from a publishing medium to an interactive platform for the delivery of personal services enabled electronic commerce, electronic government, and many other rich and diverse online interactions, from electronic health and electronic learning to social networks and the broader participative web. The possibility for individuals to establish a personalised interaction with, and to be recognised by, a remote computer system has been a major step. It has ushered in a decade of innovation, enabling Internet services to become pervasive, ubiquitous and increasingly essential in everyday life. It has transformed our economies and societies, serving as a building block for the Internet economy.

デジタル ・アイデンティティ・マネジメントはどのように機能するのか？
How does digital identity management work?

デジタル・アイデンティティ・マネジメントは組織と個人との間で信頼できる遠隔対話

[62] OECD, 2008a, page 4. See also OECD, 2008b.

（リモートインタラクション）を可能にする[63]。デジタル・アイデンティティ・マネジメントのライフサイクルはいくつかのプロセスを含む[64]。

The management of digital identity enables trusted remote interactions between an organisation and an individual. Managing the digital identity lifecycle generally involves several processes:

i) システムによって個人が認知される（known）ためには、個人は、まずシステムに登録しなければならない。個人のアイデンティ又はアイデンティティ属性（identity attributes）に関する状況（conditions）についてチェックされ、そして、クレデンシャル（credentials）のセットがシステムから提供される。これがいわゆる「登録（registration）」又は「加入（enrolment）」プロセスである。

In order to be known by the system, the individual must first register with it and the conditions related to his/her identity or identity attributes must be checked so he/she can be provided with a set of credentials; this is the so-called *registration* or *enrolment* process;

ii) その組織のリソース（resources）にアクセスするための適切な権限（permissions）及び特権（privileges）は、個人それぞれに割り当て（assigned）られる。このプロセスは通常、「認可（authorisation）」と呼ばれる。

Appropriate permissions and privileges to access the organisation's resources must be assigned to the individual, a process often called *authorisation*;

iii) リソースにアクセスするため、個人は検証することができるアイデンティティ要求をする。つまり、個人は登録プロセスで与えられたクレデンシャルを用いてシステムにログインする。この「認証（authentication）」プロセス[65]はユーザーのアイデンティティの信用性を確立させる。

To access resources, the individual makes an identity claim that can be verified: he/she logs into the system with the credentials provided during the registration process. This *authentication* process establishes confidence in the user's identity;

iv) 認証プロセスの結果は「アクセスコントロール（access control）」と呼ばれるプロセスで使われる。そこでは、システムは当該個人がリソースにアクセスするのに適切な権限を持っているかチェックする。

The result of the authentication process is used in a process called *access control*, whereby the system checks that the individual has the appropriate authorisation to access the resource;

v) 個人が当該システムとの関係を断ち切る際は、「失効」プロセスが発生し、個人のクレデンシャルはこの失効プロセスを通じて破棄される。

When the individual is not associated anymore with the system, a *revocation* process

---

63 Third parties can also be involved, for example, when identity providers participate in the registration process.

64 Authorisation and access control processes can also be considered as belonging to access management" rather than to "digital identity management".

65 The authentication process is further detailed in OECD, 2007a.

must take place whereby his/her credentials are rescinded.

デジタル ・アイデンティティ・マネジメントはなぜ経済的及び社会的デジタル相互作用に不可欠なのか？
Why is digital identity management essential for economic and social digital interactions?

上記のプロセスは実世界に既に存在するものだが、たいていの場合、その存在に注意が払われることはない。例えば、銀行口座を開設しようとすると私たちのアイデンティティを証明するクレデンシャルの見せるように要求される、私たちは雇用主の施設の敷地内に出入する際に社員証を提示し、私たちは総選挙で投票するために身分証明書を提示し、私たちはアルコール飲料を購入したい時に年齢を証明しなければならない。実世界におけるアイデンティティ・マネジメントは人々の相互作用におけるリスク対処を支援し、集団の相互作用において信用を増大させる。それゆえ、デジタル・アイデンティティ・マネジメントは経済的および社会的生活において重要なものである。実体とデジタル・アイデンティティ間の明白なつながりが乏しく、それによってオフラインにはない追加の不確実性がもたらされるオンラインという場所でも同じことが言える。

These processes already exist in the physical world, but in many instances, we do not pay attention to their existence: for example, when we want to open a bank account and are asked to show credentials to prove our identity; when we use our employee badge to enter the premises of our employer's facilities; when we show an identity document to vote at national elections; or when we want to buy alcohol and have to prove our age. Identity management in the physical world helps address risks associated with human interactions and increases confidence between the parties interacting. It is therefore fundamental for economic and social life. The same is true online, where the lack of a demonstrable link between a physical person and a digital identity can create additional uncertainties that do not exist offline.

公共政策におけるもっとも大切なこととは、経済的及び社会的オンライン相互作用への移行や信頼に基づくデジタルサービスを創出させるような革新をもたらすインターネットの経済的及び社会的潜在的可能性を十分に認識させる有効かつ効率的なデジタル・アイデンティティ・マネジメント戦略の開発である。

What is at stake from a public policy point of view is the development of effective and efficient digital identity management strategies to fully realise the economic and social potential of the Internet by migrating economic and social interactions online and unleashing innovation to create trust-based digital services.

ユーザーに対するデジタル・アイデンティティ・マネジメント戦略の利益とは何か？
What are the benefits of digital identity management to users?

デジタル・アイデンティティ・マネジメントは、自身のリソースへのアクセスを認める

組織のセキュリティにとって不可欠な要素である。また、それらリソースへアクセスをする個人のセキュリティにとっても不可欠なものである。その人自身に関わること（例えば、銀行にある資金や医療記録のような個人データ）ではなおさらである。セキュリティとプライバシー提供によって、デジタル・アイデンティティ・マネジメントは離れた集団間で信頼形成を可能にさせる。

Digital identity management is essential to the security of the organisation that grants access to resources in its information system. It is also essential to the security of the individual who accesses these resources, particularly when they belong or relate to him/her (e.g. money in a bank, or personal data such as a medical record). By offering security and privacy, digital identity management enables the establishment of a trusted relationship between remote parties.

デジタル・アイデンティティ・マネジメントは、完全保証もしくは無保証といったような二択を提供することはしない。デジタル・アイデンティティ・マネジメントは、（例えば低・中・高のように）適正にあわせて、保証レベルの幅を提供する。保証レベルに選択幅を持たせるという理論的根拠は、集団間での相互作用で生じるリスクレベルからもたらされる。もし保証レベルがリスクレベルより低いならば、集団間は互いに作用しそうにない（例えば保証レベルが低程度では、経済的価値の高い取引を保護することはできないだろう）。反対に、個人にあまりにも高い保証レベルを提供させるようにすることは、高い保証レベルを要求しない中程度や低程度のリスクにある取引から彼らを引き離すかもしれない。実際、現実の世界においては、私たちは、その作用に伴ったリスクレベルによって正当化されるときに、私たちのアイデンティティの証明を要求されたり、アイデンティティ属性を提出したりしている。アイデンティティ情報や無限の取引記録（transaction record）を記録する情報システムの能力からして、（保証レベルとリスクレベルの）確かな均衡はオンラインではなおさら重要である[66]。

Digital identity management does not offer a binary choice between full assurance or no assurance regarding the parties to an interaction. It offers a range of levels of assurance, as appropriate (e.g. low, medium or high). The rationale for selecting the level of assurance primarily includes its alignment with the level of risk carried by the interactions between the parties. If the level of assurance is lower than the level of risk, the parties are likely not to interact (e.g. a low level of assurance will not enable to secure a high value transaction). Reversely, asking individuals to provide too high a level of assurance might deter them from carrying out medium or low risk interactions, which do not seem to demand it. Indeed, in the physical world, we are used to being asked to prove our identity or to exhibit identity attributes when it is justified by the level of risk involved in a given interaction. Ensuring proportionality is even more important online because of the capacity of information systems to store identity information and transaction records indefinitely.

---

[66] Practically, however, the assessment of the level of risk for an interaction depends on many factors including the value of the transaction, the context in which it takes place but also the amount of risk that the parties are accepting to take (i.e. “risk appetite”). It is therefore possible that the parties will disagree on what level of assurance is most appropriate or that similar transactions will require different levels of assurance when carried out by different parties.

さらに、場合によっては、オンラインサービスの提供はオフラインよりも高程度のプライバシー保護を可能にする。例えば、現実世界では、個人の身元を明らかにすることなしに年齢や婚姻歴といったアイデンティティ属性を確認することや、シュードニムの使用に基づいた法的拘束力のある信頼されたオフラインの相互作用を確立することは困難である。しかしながらこのようなプライバシー保護メカニズムはオンラインで可能である。

Furthermore, in some cases, the delivery of services online enables a higher degree of privacy protection than what is possible offline. For example, it is difficult in the physical world to validate identity attributes like age or marital status without identifying an individual or to establish legally binding trusted offline interactions based on the use of pseudonyms. Such privacy protective mechanisms are however possible online.

技術によって可能となる最高レベルのプライバシー保護を確実にしつつ、適切な保証レベと一致していることが、特に中・高価値のオンラインサービス市場開拓にはきわめて重要なことである。

Ensuring the highest level of privacy protection that technology enables, consistent with the appropriate level of assurance, is critical to further developing the market for online services, and in particular medium and high value ones.

政策課題は何か？

What are the policy challenges?

デジタル・アイデンティティ・マネジメントは、オフラインサービスからオンラインへの移行、新しいデジタルサービスの創造などの入り口ランプ（access ramp）を提供してきた。そして、まだ進歩の余地がある。

While digital identity management has provided the access ramp to the online migration of offline services and to the creation of new digital services, there remains room for progress.

- 一点目として、現在の多くのデジタル・アイデンティティ・マネジメントの実装では、限界がある。その限界は、インターネット経済開発へのプラスの成長を妨げるかもしれない。

  First, many current digital identity management practices have limitations that may impede their continued positive impact on the development of the Internet economy.

  サービス・プロバイダーとの契約において、個人はサービスの利用を始める前に登録プロセスを経なければならない。したがって毎回、個人は登録プロセスで作られる適切なクレデンシャル（例えば、最低限、ログイン ID とパスワードのような共通秘密）を用いた認証を受けなければならない。サービスが増えると同時に個人の登録は増加し、増える個人のクレデンシャル管理の複雑さが障害となる。もし、クレデンシャルの合計がユーザーの限度に達して、新しいサービスへの変更を嫌悪させるならば、すでに確立されたサービ

ス・プロバイダーによる不公平な利益をもたらすことになるだろう。同様に、もしユーザーが簡単さや便利さというものを選択して、覚えやすい貧弱なパスワードの利用をしたり、ひとつのパスワードが危険にさらされれば直ちにアカウントの大部分を危うくさせるようなサービスをまがってのパスワードの再利用をしたりするならば、セキュリティの脆弱性を引き起こす。ユーザーは、安全性のないファイルや一枚の紙切れで一緒くたにパスワードを管理することがあり、同時に侵入者がつけ込む「単一障害点」を作り出す。

To interact with service providers, individuals have to register before they can start using a service and, each time thereafter, they have to be authenticated with the appropriate credentials created in the registration process (e.g. minimally, a login identity and a shared secret such as a password). As individuals increasingly register with a growing number of services, the complexity of managing ever more personal credentials becomes an impediment. It may create an unfair advantage for well-established service providers if users hesitate to join new alternative services to limit the total number of their credentials. Likewise, it can generate security weaknesses if users opt for easy-to-remember but weak passwords and/or reuse them across many services, creating a vulnerability in most of their accounts as soon as one is compromised. Users may also keep their passwords together in an insecure file or on a piece of paper, creating a "single point of failure" that an intruder can exploit.

- 二点目に現在使われているオフラインサービスに広く行きわたった多くのデジタル・アイデンティティ・マネジメントの実装は、高レベルのリスクを伴った経済的価値の高いサービスの開発を支えるための十分な強固さがない。

  Second, many widespread digital identity management practices currently in use are not robust enough to support the development of higher value services which carry a higher level of risk.

  インターネット利用の初期段階から、オフラインサービスのオンライン提供の数は増え続けている。しかしながら、オンラインでは利用できないサービスは多くある。なぜなら、それらサービスは現在提供されているデジタル・アイデンティティ・マネジメントの実装よりも高い保証レベルを求めているからである。

  The number of offline services offered online has kept increasing since the early days of the Internet. However, a number of services are not yet available online because they require a level of assurance which is higher than what most digital identity management practices currently enable. Three main factors explain this situation:

  - サードパーティーは、集団の取引では高程度の保証レベルの提供することが要求される。しばしば「アイデンティティ・プロバイダー」と呼ばれるこのサードパーティーは、個人の登録、識別性の確保、クレデンシャルの発行といった業務の実行に責任がある。これら実行のコストは比較的に高いので、一般的に高レベルの保証をするア

イデンティティ・プロバイダーの存在は、市場原理においては重要であるとは思われない。

A third party has often been considered o provide a high level of assurance regarding parties to an interaction. This third party, often called an “identity provider”, is responsible for carrying out the registration of the individuals, for establishing their identity, and for issuing credentials. As the cost of these operations is relatively high, market forces do not seem to be sufficient for general high assurance identity providers to emerge, although there are some niche examples.

- さらに、高程度の保証レベルのサービスは、アイデンティティのチェックのために政府によって「証明された（certified）」情報、たとえば、ID カード、運転免許証、パスポート、社会保障カード、出生証明書、婚姻証明書などの提出を要求する。そのような証明書がオンラインで責任をもって提供するメカニズムがない中では、高程度の保証レベルのサービスの展開では、オフラインでの手作業のプロセスが必要となる。この費用のかかるステップが、デジタル・アイデンティティ・マネジメントのプロセスにかかる全体的な経済効果や、高価値なサービスのオンラインへの移行を妨げる。

  −Moreover, to check an identity claim, high level of assurance services often require government “certified” information included in an identity card, driver’s license, passport, social security card, birth certificate, marital status certificate, etc. Where no reliable mechanism exists to provide such elements online, the delivery of high level of assurance services requires an offline manual process. This expensive step impedes the overall economic efficiency of the digital identity management process and the online migration of high value services as much as it prevents the creation of new digital services.

- 最後に、強固な認証クレデンシャルの個人利用がクリティカル・マス（ある商品やサービスの普及率が一気に跳ね上がるための分岐点）に達するまでサービス・プロバイダーは新しいサービスへの投資を保留する。一方、個人は強固な認証が要求されるサービスがクリティカル・マスに達するまで、強固な認証クレデンシャルの利用をとどめている。

  Finally, a circular situation exists whereby on the one hand, service providers are holding back from investing in new services until a critical mass of individuals use strong authentication credentials and, on the other hand, individuals are waiting for a critical mass of services that require strong authentication before they adopt the technology.

- 三点目に、高レベルなアイデンティ保証を提供するデジタル・クレデンシャルは国際的に認められておらず、クロスボーダーの高価値な取引を妨げられている。

Third, digital credentials providing a high level of identity assurance are not internationally recognised, preventing cross-border high value interactions.

政府の役割は何か？
What is the role of governments?

多くの経済的および社会的な関係者が低、中、高程度の保証レベルのクレデンシャルを提供している一方で、政府が個人の ID 属性、例えば、名前、市民権、生年月日、家族関係（血縁、婚姻など）といった情報の、最も信頼できる第一の発行主体である。

While many economic and social actors provide low, medium and high level of assurance credentials, governments are generally the primary issuers of the most trustworthy credentials for individuals' identity attributes such as their name, citizenship, date of birth, civil status (parenthood, marital status, etc.).

政府が発行するクレデンシャルの形は国ごとに異なっているが、それらクレデンシャルは一般的に経済的価値の高い公共および民間サービスの利用を可能にする。オンラインサービスへの移行や創造力に富んだ経済的価値の高いデジタルサービスの発展のために、市場関係者は一貫（end to end）したデジタル・アイデンティティ・マネジメント・プロセスの構築を必要としている。それゆえ、政府がデジタル形式での ID 属性に関する証明書の提供ツールやプロセスを提供していないという事実は障壁となっている。その障壁は政府が取り払うことのできるものである。

Although the form of these government issued credentials varies across countries, they generally enable high value public and private services offline. To migrate such services online and foster the blossoming of innovative digital high value services, market players need to establish end-to-end digital identity management processes. Therefore, the fact that a process or a tool provided by the government is not available in a digital form is currently a barrier which only governments can remove.

加えて、全国民に対する本質的なオンラインサービスの提供役としての政府は、経済的価値の高いサービスをクリティカル・マスにし、そして個人の高程度の保証レベルのクレデンシャル管理や保持をクリティカル・マスにする支援をする能力がある。政府が規範となり、ユーザーフレンドリーなデジタル・アイデンティティ・マネジメント・ソリューションの出現のための環境を政府自身が創出することを政府は実装できる。政府は、全ての利害関係者のために長期的実行可能性のある好景気や規制条件を創出する柔軟性のある政策を増進させることで、リーダーシップをとることができるし、促進の働きをするものとして動くこともできる。そして最終的に政府はジタル・アイデンティティ・マネジメントの実践が可能の限り個人のプライバシーを尊重するテクノロジーをうまく活用することを保証する責任がある。

In addition, governments have the capability, as providers of essential online services to the whole population, to help generate a critical mass of high-value services and a critical mass of

individuals equipped and trained to manage a high level of assurance credentials. Acting as model users, they can establish practices for themselves which can create the conditions for the emergence of user-friendly digital identity management solutions. Governments can take leadership and act as catalysts, promoting flexible policies for all stakeholders and creating favorable market and regulatory conditions for long term viability. Finally, governments also have a responsibility to ensure that digital identity management practices take advantage of technologies to enhance individuals' privacy where possible.

現在、政府はデジタル・アイデンティティのマネジメントのための国家戦略の開発と実装している[67]。より良いポリシー選択は、今日のインターネット経済のさらなる発展を可能にし、市場に長期間の良い影響を与える。

Governments are currently developing and implementing national strategies for the management of digital identity. Making good policy choices today can positively influence the market in the long run and enable the further development of the Internet economy.

2. 政府のための政府ポリシーへの指針

II. Policy guidance for governments

政府方針の指針は以下の事柄の認識を基礎としている。

The principles below are based on the recognition that:

- アイデンティティ・マネジメントは、オンラインでも実世界でも、信頼性のある取引提供のためには必須である。
  Identity management is essential to provide trusted interactions between parties in the online and the physical worlds.

- デジタル・アイデンティティ・マネジメントは、インターネット経済の発展に必須であり、デジタル・アイデンティティ・マネジメントは、i）低、中および高価値なオンライン公共および民間サービスの革新、ii）組織のリソースのより効率的な利用の支援、そして、iii）オンラインでのユーザーの利便性の改善によって、多くの経済的および社会的利益をもたらすものである。
  Digital identity management is critical to the development of the Internet economy and brings considerable economic and social benefits by *i)* enabling innovative low, medium and high value online public and private services; *ii)* supporting the more efficient use of organizational resources; and *iii)* improving user convenience online.

- 現実世界に存在するような信頼があり高価値である経済的･社会的活動をデジタル世界でも発展させることが、長期的な目標である。
  The development in the digital world of high-value trust-based economic and social activities that exist in the physical world is an important policy objective.

---

[67] See OECD (2011), National Strategies and Policies for Digital Identity Management in OECD countries, http://dx.doi.org/10.1787/5kgdzvn5rfs2-en.

- 政府は、信頼があり高価値である経済的・社会的なオンライン取引を促進させることができる。政府は高程度の保証レベルを可能にする提供役であり、一貫したアイデンティティ・マネジメントの実装を求める市場関係者を支援する推進役である。
  Governments can facilitate high-value trust-based economic and social interactions online as providers of essential means for enabling high level identity assurance and as a driving force to help market players adopt consistent identity management practices;

- 高価値のオンラインサービスをサポートするアイデンティティ・マネジメントの実装は、インターネットアクセスが市民の一部でも困難である限り、オフラインサービスにとって代わるべきではない。
  The development of identity management practices that support high-value services online should not replace their offline counterparts, so long as Internet access remains a challenge for some citizens.

政府はデジタル・アイデンティティ・マネジメントの明確な国家戦略を採用すべである。
Governments should adopt a clear national strategy for digital identity management

デジタル・アイデンティティ・マネジメントの明確な国家戦略は、オフラインの経済的・社会的サービスのデジタル世界への移行、革新的なオンラインの公共および民間サービスの創造、インターネット経済の継続的発展には必須である。
A clear national strategy for digital identity management is essential to the further migration of existing offline economic and social services to the digital world, to the creation of innovative online public and private services, and therefore to the continued development of the Internet economy.

企業、市民、そして政府を含め、社会全体としての利益、および信頼されたオンライン相互作用を傷つけるようなリスクの最小化を達成すべきである。戦略開発のためのプロセスは全ての利害関係者が含まれるべきである。
It should aim to benefit the society at large, including businesses, citizens and the government, and minimise the risks that undermine trusted interactions online. The process for developing the strategy should be inclusive of all stakeholders with a view to identify and take into account their needs.

広範囲にわたるインターネット経済の潜在的な長期利益を視野に入れるべきである。
The potential long-term benefits to the broader Internet economy should be kept in sight

政府は、例えば高価値な公共または民間サービスのオンラインへの移行などの長期的な目標の必要性と達成の複雑さを理解すべきである。政府は長期目標と長期目標を達成する

手段である中期・短期的目標を区別するべきであり、長期的目標の達成を妨げる短期間のソリューションを避けるべきである。アイデンティティ・マネジメントは分野横断であり、多くの関係者を巻き込んでいるので、小さな変化は広範囲に影響が及ぼされるものであって、段階的に増加させる全ての利害関係者を巻き込んだアプローチは、長期的成功を確証させる必要がある。

Governments should recognise the need for and the complexity of achieving long term objectives such as the migration online of public and private high-value services. They should clearly distinguish these long term objectives from short and medium term means to accomplish them. They should also avoid short term solutions which could impede the achievement of the long term goals. As identity management is a crosscutting area, involving many participants, and where small changes can have wide-ranging implications, a phased incremental policy approach involving all stakeholders may be needed to ensure long term success.

国家戦略が電子政府にフォーカスされているならば、政策は、必要に応じて、以下のこと含みつつ、長期・中期の経済的・社会的な利益を拡張されるようにデザインされるべきである。

Where the national strategy is focused on e-government, policies should be designed to extend the benefits to the rest of the economy and society in the medium and long term, including by, as appropriate:

- 高程度の保証レベルのメカニズムをベースにした高価値なサービスのクリティカル・マスに加えて、高程度の保証レベルのクレデンシャルの個人利用もクリティカル・マスに達成させる支援

  Helping reach a critical mass of high value services based on high level of assurance mechanisms and a critical mass of individuals using high level of assurance credentials.

- 国家レベルでのデジタル・アイデンティティ・マネジメントの協調点を提供する明確なフレームワークの支援

  Supporting a clear framework providing a degree of harmonisation for digital identity management at the national level.

- 将来の技術的な発達を活かすための十分に柔軟なデジタル・アイデンティティ・ソリューションの促進 : 幅広いインターネット経済の革新を規制もしくは抑制させる政策の回避

  Promoting digital identity solutions that are sufficiently flexible to take advantage of future technical developments; Avoiding policies which can restrict or inhibit innovation within the broader Internet economy.

- 非政府のアイデンティティ・ソリューションと電子行政のデジタル・アイデンティティの相互運用性の育成

  Fostering interoperability of e-government digital identity with non-governmental identity solutions.

既存のオフライン・アイデンティティ・マネジメントの実装から始めるべきである。
Existing offline identity management practices could be a natural starting place

政府のアイデンティティ・マネジメント政策と実践は、その国の歴史、文化、政府の形態に深く根付いている。デジタル・アイデンティティ・マネジメントに関する政府戦略は、既にあるその国のアイデンティティ・マネジメント・システムの上に、必要に応じた進化を導入しながら、考慮すべきである。オフラインのアイデンティティ・マネジメント政策や実践が確立されていない国ではデジタル世界への移行はより複雑になる。

Government identity management policies and practices are deeply rooted in countries' history, culture and style of government. Most government strategies for digital identity management can therefore consider building upon their existing identity management system, introducing evolutions where appropriate. For countries without established offline identity management policies and practices, the migration to the digital world is likely to be more complicated.

現在のオフライン・アイデンティティ・マネジメントの政策と実装が効果的でないならば、オンライン移行に先だってそれらは改良されるべきである。例えば、政府は、オフライン・アイデンティティ・マネジメントをアイデンティティ・データ収集の最小化（最小化は適切な保証レベルを確実なものにするのに技術的に必須ではないが）を促進させプライバシー保護を改善するオンラインへの移行をうまく利用するべきである。

Where current offline identity management policies and practices are not considered effective, they should be improved as they are migrated online. For example, governments should take advantage of migrating offline identity management practices online to improve privacy protection through encouraging the minimisation of identity data collection where it is not technically required to ensure an appropriate level of assurance.

政府は既存のオフライン・アイデンティティ・マネジメントの政策や実装からオンラインへの移行はオフライン環境で起きる同じ問題が発生しやすいということを考慮しなければならない。例えば、アイデンティティ・マネジメントのクロスボーダーの障壁はオンライン移行によっても解決は簡単ではないだろう。同様に、デジタル・アイデンティティ・マネジメントの政策は、オフラインのアイデンティティ・マネジメントと同じように、詐称やその他不正な活動に対して取り組む必要がある。

Governments should recognise that the migration online of existing offline identity management policies and practices is likely to carry with it some of the same challenges that existed in the offline environment. For example, barriers to cross-border identity management will not be solved simply by migrating online. Similarly, digital identity management policies will have to address fraud and other malicious activities just like their offline counterparts.

電子政府の活動は国家戦略と足並みをそろえなければならない。
E-government activities should be aligned with the national strategy

デジタル・アイデンティティ・マネジメントは政府の中では分野横断的なものである。

国家戦略を最大限効果的にするためには、電子政府の活動やサービスの特異性にかかわらず、アイデンティティ・マネジメントの政策と実装が政府全域で調整されるべきである。
Digital identity management is a cross-cutting subject within the government. In order for a national strategy to be fully efficient, identity management policies and practices should be co-ordinated across the government, regardless of the specificity of each e-government activity and service.

バランスの取れたデジタル・クレデンシャルの政策は常に求められなければならない。
A balanced digital credentials policy should be sought

国家戦略は、個人が公共や民間サービスにわたり利用するデジタル・クレデンシャルの数の制限することや削減することを目標とすべきである。
The national strategy should aim to reduce or limit the number of digital credentials that individuals have to use across public and private sector services.

全てのデジタル相互作用にとって全世界的にユニークなクレデンシャル（このようなクレデンシャルはプライバシーの観点からセンシティブではある）の生成とオンラインの革新を妨げるかもしれないクレデンシャルの増加の間でバランス点を見つけるべきである。ユーザーの利便性は、例えば、低程度の保証レベルで使われるクレデンシャルの削減を促進したり、ユーザーが利用に関してクレデンシャルや保証レベルを選択することができる（いわゆる、ユーザー中心の）アプローチを促進したり、高程度の保証レベルで提供されているクレデンシャルの採択を助長したりすることで、強化される。クレデンシャルの数の削減はプライバシー保護を犠牲にすべきではなく、プライバシーに優しい技術のために行われるべきである。
A balance should be found between the establishment of a unique universal credential for all digital interactions – which is sensitive for privacy reasons - and the multiplication of credentials that may impede usability. User convenience could be enhanced, for example, by encouraging the reduction of the number of credentials used for lower level of assurance interactions, by encouraging approaches where users have the choice of what credentials and level of assurance to use (so-called user-centric approaches), or by fostering the adoption of credentials providing a high level of assurance. The reduction of the number of credentials should not take place at the expense of privacy protection but should rather be based on privacy-friendly technologies.

デジタル・アイデンティティ・マネジメントの政策はセキュリティとプライバシーの両方を保証すべきである。
Policies for digital identity management should ensure both security and privacy

集団間に関与するアイデンティティを考慮する保証レベルは取引のリスクレベル評価に

基づくべきである。
The level of assurance regarding the identity of the parties involved should be based on an assessment of the level of risk in the transactions.

信頼の構築するために、デジタル・アイデンティティ・マネジメントの実装と要件は集団間の取引におけるリスクレベルに比例されるべきである。デジタル・アイデンティティ・マネジメントの実装におけるプライバシー上の潜在的影響は適切な評価と対処がなされるべきである。
To establish trust, digital identity management practices and requirements should be proportionate to the level of risk in the interactions between the parties. The potential impact on privacy of digital identity management practices should be assessed and addressed as appropriate.

デジタル・アイデンティティ・マネジメントの実装は法律上のプライバシー保護要件に尊重すべきである。デジタル・アイデンティティ・マネジメント・システムの発展と実施は着手の段階からデータセキュリティを含めてプライバシー保護をつめるべきである。プライバシーとセキュリティの両方を支援するためのテクノロジーの潜在的可能性を活かしつつ、適切なシュードニムの活用を含めて、可能な限り、革新的な技術的保護基準はプライバシー保護要求を強化しなければならない。
Digital identity management practices should respect legal privacy protection requirements. The development and implementation of digital identity management systems should include privacy protection, including data security, from the outset. Taking advantage of the potential for the technology to support both privacy and security, innovative technical protection measures should reinforce privacy protection requirements wherever possible, including through the use of pseudonyms where appropriate.

政府はクロスボーダーなデジタル・アイデンティティ・マネジメントを機能させるべきである。
Governments should work together to enable cross-border digital identity management

電子行政、e コマース、その他国境を越えたデジタルサービスの高価値を促進させるデジタル・アイデンティティ・マネジメントの可能性は様々な障害によって妨げられる。政府や他の利害関係者はこれら障害を削減または最小化させるように働かなければならない。政府や利害関係者は、例えば、地域的・国際的な技術基準の活用を通して、国家のデジタル・アイデンティティ・マネジメントの相互認証をより発展させたり、相互運用の環境を創出したりするために、協力すべきである。
The potential for digital identity management to facilitate high value e-government, e-commerce and other digital services across borders is impeded by various obstacles. Governments and other stakeholders should work towards reducing or minimising these obstacles. They should co-operate to further develop mutual recognition of national digital identity management approaches and to create the conditions for interoperability, for example through the use of regional and international standards.

REFERENCES

On digital identity management and electronic authentication

OECD (2007a), "OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication". Available at *www.oecd.org/dataoecd/32/45/38921342.pdf.*

OECD (2007b), "Report of the OECD workshop on digital identity management. Trondheim, Norway, 8-9 May 2007". Available at *www.oecd.org/dataoecd/30/52/38932095.pdf.*

OECD (2009), "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Maker". Available at *www.oecd.org/dataoecd/55/48/43091476.pdf.*

OECD (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing. doi: 10.1787/5kgdzvn5rfs2-en.

Other

OECD (1980), "OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data". Available at www.oecd.org/document/20/0,3746,en_2649_34255_15589524_1_1_1_1,00.html.

OECD (2002), "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security". Available at *www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.*

OECD (2008a), "Seoul Declaration on the Future of the Internet Economy". Available at *www.oecd.org/dataoecd/49/28/40839436.pdf.*

OECD (2008b), "Shaping Policies for the Future of the Internet Economy". Available at *www.oecd.org/dataoecd/1/29/40821707.pdf.*

5.3 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) （仮日本語訳）

この翻訳は、欧州連合出版局により EUR-Lex ウエブサイトに掲載された Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)の英語版の一部を訳したものである。日本語への翻訳の責任は、翻訳者の JIPDEC が負う。本翻訳は参考のための仮日本語訳であって、正確には原文を参照されたい。

Translated from the original English edition published by the Publications Office of the European Union on the EUR-Lex website: © European Union, http://eur-lex.europa.eu/, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
Responsibility for the translation into Japanese lies entirely with JIPDEC.

第 I 章　一般条項
CHAPTER I　GENERAL PROVISIONS

第 1 条　内容と目的
Article 1　Subject matter and objectives

1. この規則は、個人データの処理に関して個人を保護するためのルールと、個人データの自由な流通のためのルールを定める。
1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.

2. この規則は、自然人の基本的権利と自由、特に、個人データの保護における彼らの権利を保護する。
2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.

3. 個人データの処理における個人の保護を理由にして、EU 域内の個人データの自由な流通を制限または禁止してはならない。
3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

第 2 条　適用範囲
Article 2 Material scope

1. この規則は、全部または一部が自動化された手段による個人データの処理に適用される。また、ファイリングシステムの一部である、あるいはファイリングシステムの一部にすることが意図された個人データの自動化された手段以外の処理にも適用される。
1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. この規則は、以下のような個人データの処理には適用されない。
2. This Regulation does not apply to the processing of personal data:

(a) EU 法の適用範囲外の活動（特に国家安全保障に関する活動）において発生した個人データの処理

(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;

(b) EU 機関、団体、オフィス、および政府機関による個人データの処理
(b) by the Union institutions, bodies, offices and agencies;

(c) EU 条約第 2 章の適用範囲における活動を行う加盟国による個人データの処理
(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;

(d) 自然人が、全くの個人的または家庭内の活動において、何の利益も受けずに行う個人データの処理
(d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;

(e) 犯罪の防止、捜査、探知、起訴、あるいは刑事罰を科すために所管官庁が行う個人データの処理
(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

3. この規則は、指令 2000/31/EC（「電子商取引指令」）の適用を妨げるものではない。特に、その指令の第 12 条から第 15 条における仲介サービス・プロバイダーの責任に関する規則の適用を妨げるものではない。
3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

第 3 条　地理的範囲
Article 3 Territorial scope

1. この規則は、EU 域内を管理者または処理者が活動拠点とする場合における個人データの処理に適用される。
1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. この規則は、EU 域内に居住するデータの対象者の個人データに対して、EU 域内に拠点を持たない管理者が行った処理にも適用される。ただし、その処理活動は以下に関するものに限られる。
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

(a) EU 域内に居住するデータの対象者に対する商品やサービスの提供
(a) the offering of goods or services to such data subjects in the Union; or

(b) 彼らの行動の監視
(b) the monitoring of their behaviour.

3. この規則は、EU 域内に拠点を持たない管理者による個人データの処理に適用される。ただし、加盟国の国内法が国際公法によって適用される場所に限られる。
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

第 4 条　定義
Article 4 Definitions

この規則における用語の意味は以下の通り。
For the purposes of this Regulation:

(1) 「データの対象者」とは、特定された自然人、または管理者あるいはそれ以外の自然人や法人によって合理的な範囲で使用される手段をもって直接的または間接的に特定された自然人のことを意味する。特に、識別番号、位置データ、オンライン識別子の参照、またはその人物のアイデンティティに関する物理的、生理的、遺伝子的、精神的、経済的、文化的、または社会的な一つ以上の要素の参照によって特定された自然人のことを意味する。
(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 「個人データ」とは、あるデータの対象者に関するすべての情報を意味する。
(2) 'personal data' means any information relating to a data subject;

(3) 「処理」とは、個人データまたは個人データの集合に適用される、自動化された手段かどうかを問わないすべての操作または一連の操作を意味する。例えば、収集、記録、編集、構造化、格納、適合、変更、検索、参照、利用、あるいは移転による開示、公表または公表を可能なものにすること、整列や組み合わせ、消去や破壊などが挙げられる。
(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;

(4) 「ファイリングシステム」とは、機能的または地理的に集結、分散、あるいは拡散されているかどうかにかかわらず、特定の評価基準に従ってアクセスすることができる個人データのすべての構築された集合を意味する。
(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(5) 「管理者」とは、単独または他者と共同で個人データの処理に関する目的、条件、および手段を決定する自然人、法人、公的機関、政府機関、またはすべてのその他の団体を意味する。処理の目的、条件、および手段が EU 法または加盟国法によって決定される場合には、管理者または管理者を指名するための特定の評価基準は EU 法または加盟国法によって決定してもよい。
(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

(6) 「処理者」とは、管理者の代わりに個人データを処理する自然人、法人、公的機関、政府機関、またはその他すべての団体を意味する。
(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(7) 「受取人」とは、個人データが開示される対象である自然人、法人、公的機関、政府機関、またはその他すべての団体を意味する。
(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;

(8) 「データの対象者の同意」とは、データの対象者が、発言または明らかに肯定的な行動によって彼らに関する個人データが処理されることへの同意を表現するといった、すべての自由に行われる具体的、明示的、および通知されたその人物の意思表示を意味する。
(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

(9) 「個人データの侵害」とは、送信、格納、または処理される個人データについて、偶発的または違法な破壊、消失、変更、権限のない公開またはアクセスにつながるような秘密保持の違反を意味する。
(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(10) 「遺伝データ」とは、出生前の早い段階において継承または取得された個人の特性に関するあらゆる型のデータを意味する。

(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;

(11)「バイオメトリックデータ」とは、個人を一意的に特定することができる、物理的、生理的、または行動の特徴に関するすべてのデータを意味する。例えば、顔画像や指紋認証データなどが挙げられる。
(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;

(12)「健康に関するデータ」とは、ある個人の身体的または精神的な健康、あるいはその個人への公共医療の提供に関するすべての情報を意味する。
(12) ‘data concerning health’ means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

(13)「主要拠点」とは、管理者について言えば、個人データの処理の目的、条件、および手段に関し主な決定をする EU 内の設備のある場所を意味する。個人データの処理の目的、条件、および手段に関する決定が EU 内で実施されない場合には、主要設備とは、EU 内の管理者の設備における活動での主要な処理が実施される場所を意味する。処理者について言えば、「主要拠点」とは、EU 内の中央行政がある場所を意味する。
(13) ‘main establishment’ means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;

(14)「代理人」とは、この規則が定める管理者の義務について、その管理者の代わりに EU 内の監督機関やその他の団体から依頼を受け、行動するようその管理者に明示的に指名された EU に拠点を持つすべての自然人または法人を意味する。
(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;

(15)「事業者」とは、法律上の形式にかかわらず、経済活動に従事しているすべての事業体を意味する。つまり、特に、定期的に経済活動に従事している自然人、法人、共同経営会社、または協会のことを意味する。
(15) ‘enterprise’ means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;

(16)「事業グループ」とは、管理をする事業およびその管理された事業のことを意味する。
(16) 'group of undertakings' means a controlling undertaking and its controlled

undertakings;

(17) 「拘束的企業準則」とは、事業グループ内の一つ以上の第三者国における管理者または処理者への個人データの転送または転送の集合について、EU 加盟国の領内を拠点とする管理者または処理者が遵守する個人データ保護方針を意味する。
(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;

(18) 「子供」とは、すべての 18 歳未満の人物を意味する。
(18) 'child' means any person below the age of 18 years;

(19) 「監督機関」とは、第 46 条に従って加盟国によって確立される公的機関を意味する。
(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.

第 II 章　原則
CHAPTER II PRINCIPLES

第 5 条　個人データ処理に関する原則
Article 5 Principles relating to personal data processing

個人データは、以下を満たしていなければならない。
Personal data must be:

(a) データの対象者に対して合法、公正、そして透明性のある方法により処理される。
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

(b) 具体的、明示的、そして合法的な目的により収集され、その目的に合致しないやり方での追加処理は行われない。
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(c) 適切であり、関連性があり、それらが処理される目的を果たすために必要最小限の範囲に限られる。個人データを処理してもよい場合とは、個人データを含まない情報の処理では目的を果たすことができない場合だけである。
(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

(d) 常に正確で最新である。ある個人データがその処理の目的を満たすために正確ではない

場合、すぐに削除または訂正されるよう、あらゆる適正な措置を取らなければならない。
(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) 個人データを処理する目的において必要な期間に限り、データの対象者を識別できる形式に保存される。個人データが第 83 条の規則と条件に従った歴史的、統計的、または科学的な研究目的のためだけに処理され、定期的な審査を行いその格納を続ける必要性を評価するのであれば、それ以上の期間にわたり個人データを保存してもよい。
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;

(f) すべての処理操作は、この規則の規定を遵守する管理者の責任の下で行われる。
(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.

第 6 条　処理の合法性
Article 6 Lawfulness of processing

1. 個人データの処理は、以下の項目のうち少なくとも一つの項目が適用される場合にかぎり、合法とする。
1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) データの対象者が、一つ以上の具体的な目的のために、自分自身の個人データが処理されることに同意している。
(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) データの対象者が当事者である契約を履行するためにその処理が必要な場合。または、契約を締結する前に、データの対象者の依頼によって対策を講じるためにその処理が必要な場合。
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) 管理者が従うべき法律上の義務を果たすために、その処理が必要な場合。
(c) processing is necessary for compliance with a legal obligation to which the controller is

subject;

(d) データの対象者の重要な利益を保護するために、その処理が必要な場合。
(d) processing is necessary in order to protect the vital interests of the data subject;

(e) 公共の利益のために遂行される業務、または管理者に与えられた職権の行使のためにその処理が必要な場合。
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) 管理者が追求する正当な利益のためにその処理が必要な場合。ただし、特にデータの対象者が子供の場合、個人データの保護を必要とするデータの対象者の利益または基本的権利や自由が、上記の管理者の利益に優先される場合を除く。このことは、公的機関が職務の実施のために行った処理には適用しないものとする。
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

2. 歴史的、統計的、または科学的な研究のために必要な個人データの処理は、第 83 条の条件や保護条項により合法であるものとする。
2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. 第 1 項(c)(e)で言及されている処理の根拠は、以下のどちらかにおいて提供されなければならない。
3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) EU 法。
(a) Union law, or

(b) 管理者に課される加盟国法。
(b) the law of the Member State to which the controller is subject.

加盟国法は、公共の利益となるような目的に沿ったものでなければならない。または、加盟国法は、他者の権利と自由を保護するために必要であり、個人データの保護に関する権利の本質を尊重し、そして追求すべき正当な目的にふさわしくなければならない。
The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

4. 個人データに追加的な処理を実施する目的が、個人データを収集した目的とは異なる場合には、その処理は、第 1 項(a)から(e)のうち少なくとも一つの法的根拠に基づいていなけ

ればならない。特にこのことは、一般契約の条件のあらゆる変更に適用されるものとする。
4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

5. 第 1 項(f)について、子供に関する個人データの処理など、様々な分野やデータ処理の状況に関する条件をより具体的にするために、第 86 条に従って委任決議を採択する権限が委員会に与えられる。
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

第 7 条　同意の条件
Article 7 Conditions for consent

1. 管理者は、データの対象者が自身の個人データが定められた目的のために処理されるということに同意していることの立証責任を負うものとする。
1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.

2. データの対象者の同意が別の案件を含む書面において与えられる場合には、その同意の要件がその別の案件と区別できる方法によって明示されなければならない。
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.

3. データの対象者本人は、いつでも同意を取り下げる権利があるものとする。また、同意の取り下げは、取り下げる前の同意に基づく処理の合法性になんら影響を与えない。
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. データの対象者の立場と管理者のそれとの間に大きな不均衡がある場合には、同意は処理のための法的根拠にはならない。
4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

第 8 条　子供の個人データの処理

Article 8 Processing of personal data of a child

1. この規則の目的に則って、情報化社会のサービスを子供に直接提供する場合には、13 歳未満の子供の個人データの処理は、その子供の親または後見人が同意または許可した場合に限り合法であるものとする。管理者は、活用可能な技術を考慮に入れて、検証可能な同意取得のための相応の努力をしなければならない。
1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

2. 第 1 項は、子供についての契約の正当性、成立、または効力に関するルールの妥当性に対して、加盟国の一般契約法に影響を与えない。
2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

3. 第 1 項の検証可能な同意取得のための手段について、基準や要求条件をより具体的にするために、第 86 条に従って委任決議を採択する権限が委員会に与えられる。その際、委員会は、小規模事業および中小事業のための具体策を検討する。
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

4. 委員会は、第 1 項で示された検証可能な同意取得のための具体的手段に関する標準フォームを作成してもよい。それに関する施行法は、第 87 条(2)に示された審査手順によって採択される。
4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 9 条　特別カテゴリーの個人データの処理
Article 9 Processing of special categories of personal data

1. 人種、民族的、政治的思想、宗教、信念、労働組合員資格を明らかにするような個人データの処理、および、遺伝データまたは健康、性生活、刑事上の有罪判決、あるいは関連するセキュリティ対策についてのデータの処理は禁止する。
1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data

concerning health or sex life or criminal convictions or related security measures shall be prohibited.

2. 第 1 項は、以下の場合には適用されない。
2. Paragraph 1 shall not apply where:

(a) データの対象者が、第 7 条、第 8 条に示された条件の対象となる彼らの個人データの処理に同意した場合。ただし、EU 法または加盟国法が、第 1 項で示した禁止事項をそのデータの対象者が解除してはならないと定めている場合を除く。
(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or

(b) 適切な保護条項を与える EU 法または加盟国法でそれが認可されていて、雇用法の分野において管理者の特定の権利を行使し、義務を果たすために処理が必要な場合。
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or

(c) データの対象者が物理的または法的に同意を与えることができないとき、データの対象者または他者の重要な利益を保護するためにその処理が必要な場合。
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or

(d) 政治、哲学、宗教、または労働組合にかかわる目的を持つ財団、協会、または他のすべての非営利団体による適切な保護条項を備えた正当な活動において、その処理が実行される場合。ただしその処理は、そのメンバー、その団体の前メンバー、またはその目的においてその団体と定期的に接触をしている人々に関する処理であり、データの対象者の同意なく団体の外でデータが開示されないということを条件とする。
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profitseeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or

(e) データの対象者が明示的に公開した個人データの処理。
(e) the processing relates to personal data which are manifestly made public by the data subject; or

(f) 法的要求の立証、行使、または擁護のためにその処理が必要な場合。
(f) processing is necessary for the establishment, exercise or defence of legal claims; or

(g) データの対象者の正当な利益を保護するための手段を備えた EU 法または加盟国法に基づき、公共の利益のための職務の実行において、その処理が必要な場合。

(g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or

(h) 健康に関するデータの処理が、健康の目的のために必要であり、第 81 条の条件および予防的手段を満たしている場合。
(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or

(i) 第 83 条の条件および保護条項を満たしている歴史的、統計的、または科学的な研究のために、その処理が必要な場合。
(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or

(j) 適切な予防的手段を備えた EU 法または加盟国法で認められていて、管理者に課される法律上または規制上の義務を果たすためあるいは重要な公共の利益のために職務を実行するためにその処理が必要、あるいは職権の管理下において、刑事上の有罪判決または関連する安全対策についてのデータが処理される場合。刑事上の有罪判決に関する完全な記録は、職権の管理下においてのみ保持される。
(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.

3. 第 1 項および第 2 項の適用外項目に言及されている特別カテゴリーの個人データの処理について、評価基準、条件、および適切な保護条項をより具体的にするために、第 86 条に従って委任決議を採択する権限が委員会に与えられる。
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.

第 10 条　特定できない場合の処理
Article 10 Processing not allowing identification

管理者によって処理されたデータについてその管理者が自然人を特定することができない場合、管理者は、この規則の条項に従うためだけに、データの対象者を特定する追加的な情報を取得しなくてもよい。

If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

第 III 章　データの対象者の権利
CHAPTER III RIGHTS OF THE DATA SUBJECT

第 1 節　透明性と様式
SECTION 1 TRANSPARENCY AND MODALITIES

第 11 条　情報とコミュニケーションの透明性
Article 11 Transparent information and communication

1. 管理者は、透明性が高く容易に入手可能な、個人データの処理とデータの対象者の権利の行使に関する方針を用意しなければならない。
1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.

2. 管理者は、特に子供向けの情報については、データの対象者に個人データの処理について情報提供およびコミュニケーションを行う際、明瞭な形式に基づき、明確かつ簡単な言葉を使用し、そしてデータの対象者のレベルに合わせなければならない。
2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.

第 12 条　データの対象者の権利を行使するための手順と仕組み
Article 12 Procedures and mechanisms for exercising the rights of the data subject

1. 管理者は、第 14 条に示された情報を提供し、第 13 条および第 15 条から第 19 条に示されたデータの対象者の権利を行使するための手順を確立しなければならない。管理者は、特に第 13 条および第 15 条から第 19 条に示された対応への要求事項を容易にするための仕組みを提供しなければならない。個人データが自動化された手段で処理される場合、管理者は、電子的に要求を出すための手段も提供しなければならない。
1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and

Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.

2. 管理者は、要求事項を受け取ってから遅くとも 1 カ月以内に遅延無く、第 13 条および第 15 条から第 19 条に基づき何らかの対応がなされたのかどうかをデータの対象者に通知し、要求された情報を提供しなければならない。複数のデータの対象者が権利を行使し、管理者側の過度の不要な労力を避けるために彼らのある程度の協力が必要な場合、上記の期間をもう 1 カ月延長してもよい。この情報は書面で提供される。データの対象者が電子的形態により要求事項を出した場合、データの対象者から別の方法を求められない限り、その情報は電子的形態により提出されるものとする。

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

3. 管理者がデータの対象者の要求への対応を拒否する場合、管理者は、データの対象者に、その拒否の理由および監督機関に苦情を申し立て司法的な救済を求めることができる旨を通知する。

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

4. 第 1 項に示された要求への対応や情報提供は、無償でなければならない。その要求が明らかに度を越えている場合、特に反復して行われる場合には、管理者は要求への対応や情報提供について料金を請求してもよいし、または要求された対応を行わなくてもよい。その場合、管理者は、その要求が明らかに度を越えているということについて立証責任を負わなければならない。

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

5. 第 4 項について、明らかに度を越えた要求および料金に関する評価基準や条件をより具体的にするために、第 86 条に従って委任決議を採択する権限が委員会に与えられる。

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.

6. 委員会は、第 2 項で示された電子的形態を含むコミュニケーションの標準的手続きを指定および標準書式を作成してもよい。その際委員会は、小規模事業および中小事業のために適切な対応を取らなければならない。これら実施される活動行為は、第 87 条(2)に示された審査手順によって採択される。
6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 13 条　受取人に関する権利
Article 13 Rights in relation to recipients

管理者は、それが不可能と判明したり過度の労力を必要としたりしなければ、第 16 条と第 17 条に従って実行したすべての訂正や消去についてデータを開示した各受取人に連絡する。
The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

第 2 節　情報とデータの入手
SECTION 2 INFORMATION AND ACCESS TO DATA

第 14 条　データの対象者への情報
Article 14 Information to the data subject

1. あるデータの対象者に関する個人データが収集されるとき、管理者は、少なくとも以下の情報をそのデータの対象者に提供しなければならない。
1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

(a) 管理者の身元と詳しい連絡先。また、もし存在するのであれば、管理者の代理および Data Protection Officer（以下「DPO」）の身元と詳しい連絡先。
(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;

(b) 個人データの処理の目的。その処理が第 6 条(1)(b)に基づく場合は、契約条件および一般条件を含む。その処理が第 6 条(1)(f)に基づく場合は、管理者が追求する正当な利益を含

む。
(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

(c) 個人データが保存される期間。
(c) the period for which the personal data will be stored;

(d) データの対象者は、管理者に対し、個人データへのアクセス、個人データの修正または消去を要求する権利又は当該データの処理に異議を唱える権利を有すること。
(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;

(e) 監督機関に苦情を申し立てることができる権利、およびその監督機関の詳しい連絡先。
(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(f) 個人データの受取人または受取人の属性。
(f) the recipients or categories of recipients of the personal data;

(g) 管理者が第三国又は国際機関に転送する予定がある場合はその旨、及び委員会による十分性決定を引用した上での当該第三国又は国際機関が提供する保護のレベル。
(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;

(h) 個人データが集められる特定の環境において、データの対象者に公正な処理を保証するために必要なそれ以外のすべての情報。
(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

2. 管理者は、データの対象者から個人データを収集する場合、第 1 項に規定する情報に加え、その個人データを与えることの任意性及び当該データを与えなかった場合に当該対象者に生じる結果について、データの対象者に通知しなければならない。
2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.

3. 管理者は、データの対象者から個人データを収集しない場合、第 1 項に規定する情報に加えて、その個人データのソースについてデータの対象者に通知しなければならない。
3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.

4. 管理者は、第 1 項、第 2 項、および第 3 項で示された情報を以下の時期に提供しなければならない。
4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:

(a) データの対象者から個人データを取得したとき。
(a) at the time when the personal data are obtained from the data subject; or

(b) データの対象者から個人データを取得しない場合は、それを記録したとき又は当該データが収集もしくは処理された特定の環境を考慮した収集後の合理的な期間内。また、別の受取人への開示が考えられる場合は、遅くともデータが最初に開示されるとき。
(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.

5. 第 1 項から第 4 項は、以下の場合には適用しない。
5. Paragraphs 1 to 4 shall not apply, where:

(a) データの対象者が、第 1 項、第 2 項、および第 3 項で示された情報をすでに所有している場合。
(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or

(a) at the time when the personal data are obtained from the data subject; or

(b) データの対象者から収集されたデータではなく、かつ、そのような情報の供給が不可能だと判明したり、または過度の労力を伴ったりする場合。
(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or

(c) データの対象者から収集されたデータではなく、かつ、法によってその記録や開示が明白に定められている場合。
(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or

(d) データの対象者から収集されたデータではなく、かつ、そのような情報を提供することが、第 21 条に従った EU 法又は加盟国法で定める他者の権利と自由を侵害することとなる場合。
(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.

6. 第 5 項(b)に該当する場合には、管理者はデータの対象者の正当な利益を保護するために適切な対策を講じなければならない。
6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.

7. 委員会には、第 1 項(f)に規定する受取人の属性の基準、第 1 項(g)に規定する潜在的なアクセスの通知における要求条件、第 1 項(h)に規定する特定のセクターや状況において必要なそれ以外のすべての情報に関する評価基準をより具体化し、第 5 項(b)に定められた例外に関する条件および適切な予防的手段をより具体化するための規定に基づき委任法令を制定する権限が与えられる。そのような法令を制定するにあたり、委員会は、零細及び中規模事業者のために適切な対策を講じなければならない。
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.

8. 委員会は、必要であれば、様々な分野及びデータ処理状況の特性及び必要性を考慮に入れ、第 1 項から第 3 項で示された情報を提供するための標準形式を定めてもよい。それに関する施行法は、第 87 条(2) に規定する審議手順により制定しなければならない。
8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 15 条　データの対象者のアクセス権
Article 15 Right of access for the data subject

1. データの対象者には、当該対象者に関連する個人データが処理されるのかどうかについて、いつでも管理者に確認を要求できる権利がある。そのような個人データが処理される場合、管理者は以下のような情報を提供しなければならない。
1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:

(a) 処理の目的。
(a) the purposes of the processing;

(b) 関連する個人データの属性。
(b) the categories of personal data concerned;

(c) 特に受取人が第三国に存在する場合、個人データがこれから開示される、またはすでに

開示された受取人または受取人の属性。
(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;

(d) 個人データが保存される期間。
(d) the period for which the personal data will be stored;

(e) データの対象者は、管理者に対し個人データの修正または消去を要求する権利又は当該データの処理に異議を唱える権利を有すること。
(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;

(f) 監督機関に苦情を申し立てることができる権利、およびその監督機関の詳しい連絡先。
(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(g) 処理される個人データに関する連絡、およびそれらのソースに関するすべての入手可能な情報に関する連絡。
(g) communication of the personal data undergoing processing and of any available information as to their source;

(h) 少なくとも第 20 条に規定する判断を行う場合の、当該処理の重大性及び予想される結果。
(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.

2. データの対象者には、処理される個人データに関して管理者から連絡を受ける権利がある。データの対象者が電子形式により要求を出した場合、データの対象者に別の方法を要求されない限り、その情報は電子形式で提供されなければならない。
2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

3. 委員会には、第 1 項(g)に示された、データの対象者への個人データの内容についての連絡の評価基準と要求条件をより具体的なものにするために、第 86 条の規定に基づき委任法令を制定する権限が与えられる。
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.

4. 委員会は、様々な分野及びデータ処理状況の具体的な特徴及び必要性を考慮し、データの対象者の本人認証およびデータの対象者への個人データ転送を含め、第 1 項に規定する情報の入手の要求および承諾を行うための標準形式と手順を指定してもよい。それに関す

る施行法は、第 87 条(2) に規定する審議手順によって制定されなければならない。
4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 3 節　訂正と消去
SECTION 3 RECTIFICATION AND ERASURE

第 16 条　訂正をする権利
Article 16 Right to rectification

データの対象者には、彼らに関する個人データが不正確な場合、管理者にその訂正をさせる権利がある。データの対象者には、訂正された記述を提供するなどして、不完全な個人データを完全なものにさせる権利がある。
The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

第 17 条　忘れ去られる権利および消去する権利
Article 17 Right to be forgotten and to erasure

1. データの対象者には、以下のいずれかに該当する場合、特にその人物が子供のときに開示した個人データについて、その人物に関連する個人データの削除とそのデータの頒布の中止を管理者に実行させる権利がある。
1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

(a) そのデータを収集および処理した目的において、そのデータがもはや必要ではない場合。
(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) 第 6 条(1)(a)によりその処理の根拠となる同意をデータの対象者が取り下げた場合、または同意されていた保存期限を過ぎた場合、およびそのデータの処理について法的な根拠

が一切無い場合。
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) 第 19 条の規定に従い、データの対象者が個人データの処理に異議を唱えた場合。
(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) 当該データの処理が、その他の理由によりこの規則に準拠しない場合。
(d) the processing of the data does not comply with this Regulation for other reasons.

2. 第 1 項で規定する管理者がその個人データを公開していた場合、そのデータを処理している第三者に対してデータの対象者が個人データのコピーまたは複写へのすべてのリンクを消去するよう要求している旨を通知するなど、管理者が責任を持つデータの公開に関して技術的手段を含むあらゆる合理的手段を管理者は取らなければならない。管理者が個人データの第三者による公開を認可していた場合、管理者はその公開について責任を負うものとみなされる。
2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

3. 管理者は、以下の理由によってその個人データの保持が必要な場合を除き、遅滞なく消去しなければならない。
3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(a) 第 80 条に従って表現の自由の権利を行使するため。
(a) for exercising the right of freedom of expression in accordance with Article 80;

(b) 第 81 条に従って国民の健康に関する公共の利益を守るため。
(b) for reasons of public interest in the area of public health in accordance with Article 81;

(c) 第 83 条に従った歴史的、統計的、および科学的な研究目的のため。
(c) for historical, statistical and scientific research purposes in accordance with Article 83;

(d) EU 法または加盟国法によって管理者に課される法律上の個人データ保持義務を遵守するため。加盟国法は、公共の利益となるような目的に沿ったものであり、個人データの保護に関する権利の本質を尊重し、そして追求すべき正当な目的にふさわしくなければならない。
(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be

proportionate to the legitimate aim pursued;

(e) 第 4 項の規定に該当する場合。
(e) in the cases referred to in paragraph 4.

4. 以下の場合、管理者は個人データを消去するのではなく、その処理を制限する。
4. Instead of erasure, the controller shall restrict processing of personal data where:

(a) データの対象者が個人データの正確性について異議を申し立てており、管理者がデータの正確性について確認している期間中。
(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;

(b) 管理者はそのタスクの達成のためにもはや個人データを必要としないが、それらを証拠として保持しなければならない場合。
(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;

(c) 処理が違法であるため、データの対象者がその消去に異議を唱え、代わりにそれらの利用の制限を要求している場合。
(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;

(d) データの対象者が第 18 条(2)の規定に基づき、別の自動化された処理システムに個人データを移すよう要求している場合。
(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

5. 第 4 項の規定に該当する個人データは、保存する場合を除き、証拠とする目的のためにのみ処理することができる。また、データの対象者の同意を得た場合は、他の自然人又は法人の権利の保護又は公共の利益のために処理することができる。
Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. 第 4 項の規定に従い個人データの処理が制限される場合、管理者は、処理の制限を解除する前に、データの対象者にその旨を通知しなければならない。
Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

7. 管理者は、個人データの消去に関して定められた期限及びデータ保存の必要性に関する定期的な見直しについて定められた期限の両方又は一方が、確実に守られる仕組みを構築しなければならない。
The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8. 個人データを消去する場合、管理者はそれ以外の処理をしてはならない。
Where the erasure is carried out, the controller shall not otherwise process such personal data.

9. 委員会には以下をより具体的に示すために、第 86 条の規定に基づき委任法令を制定する権限が与えられる。
The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:

(a) 特定の分野および特定のデータ処理状況において、第 1 項を適用するための評価基準と要件。
(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;

(b) 第 2 項に規定する、一般に利用可能なコミュニケーションサービスから個人データのリンク、コピー、または複写を削除する際の条件。
(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;

(c) 第 4 項に規定する、個人データの処理を制限するための評価基準と条件。
(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

第 18 条　データのポータビリティに関する権利
Article 18 Right to data portability

1. データの対象者には、構造化された共通フォーマットにより個人データが電子的手段で処理される場合、当該対象者が別途利用可能なように電子的に構造化された共通フォーマットの形式で、処理中のデータのコピーを管理者から入手する権利がある。
1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

2. データの対象者が個人データを提供しその処理が本人の同意または契約に基づいている場合、データの対象者は、その個人データおよびデータの対象者が提供したその他の情報を保持している自動処理システムから、管理者に妨げられることなく個人データを回収し、共通の電子的なフォーマットによる別の自動処理システムに移す権利がある。
2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used,

without hindrance from the controller from whom the personal data are withdrawn.

3. 第 1 項に規定する電子フォーマット、および第 2 項の規定に基づく個人データの移転のための技術標準、様式、および手順について、委員会は具体的に指定してもよい。それに関する施行法は、第 87 条(2) に規定する審議手順によって制定されなければならない。
3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 4 節　異議を唱える権利とプロファイリング
SECTION 4 RIGHT TO OBJECT AND PROFILING

第 19 条　異議を唱える権利
Article 19 Right to object

1. データの対象者には、それぞれの状況による根拠に基づき、第 6 条(1)(d)、(e)、および(f)による個人データの処理に対していつでも異議を唱える権利がある。ただし、管理者が、その処理に関してデータの対象者の利益または基本的人権および自由に優先される正当な根拠を示した場合にはその限りではない。
1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. 個人データがダイレクトマーケティングの目的のために処理される場合、データの対象者には、そのマーケティングのための個人データの処理に対して、無償で異議を唱える権利がある。この権利は明瞭な方法によって明示的にデータの対象者に付与され、他の情報とは明確に区別することができなければならない。
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

3. 第 1 項および第 2 項による異議の申し立てが認められた場合、管理者はその個人データの使用または処理を中止する。
3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.

第 20 条　プロファイリングに基づく判断
Article 20 Measures based on profiling

1. すべての自然人は、その自然人に法的効果を生じ又は重大な影響を与える判断が、その自然人のある個人的側面の評価のため又はその自然人の特に職務実績、経済状況、位置、健康、個人的嗜好、信頼性、行動に関する分析もしくは予測のための自動処理のみに依拠しているものについては、それに従わない権利を有する。
1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

2. この規則の他の条項に準拠し、かつ以下のような処理が行われる場合に限り、その人物を第 1 項に規定する判断に従うこととすることが認められる。
2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

(a) その処理が、契約の締結または履行において行われる場合。ただし、データの対象者が契約の締結または履行を要求してそれが満たされる場合、あるいは人間を介在させる権利などデータの対象者の正当な利益を保護するための適切な手段が提示されている場合に限る。
(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or

(b) その処理が、EU 法又は加盟国法によって明確に認められており、その法にデータの対象者の正当な利益を保護するための適当な手段が定められている場合。
(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

(c) その処理が、第 7 条に定められた条件および適当な予防的手段の下でのデータの対象者の同意に基づいている場合。
(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. 自然人のある個人的側面を評価するための個人データの自動処理は、第 9 条に規定する特別カテゴリーの個人データのみに基づくものであってはならない。
3. Automated processing of personal data intended to evaluate certain personal aspects

relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. 第 2 項のような場合、第 14 条に基づき管理者が提供する情報には、第 1 項に規定する判断処理の存在およびその処理によって考えられるデータの対象者への影響といった情報が含まれなければならない。
4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. 委員会には、第 2 項で規定するデータの対象者の正当な利益を保護するための適当な手段について、その評価基準および条件をより具体的に示すために、第 86 条の規定に基づき委任法令を制定する権限が与えられる。
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph

第 5 節　制限
SECTION 5 RESTRICTIONS

第 21 条　制限
Article 21 Restrictions

1. EU 法または加盟国法では、第 5 条(a)～(e)、第 11 条～第 20 条、および第 32 条に規定する義務および権利の適用範囲を、法的措置を用いて制限してもよい。ただし、そのような制限が、民主社会において以下を守るために必要かつ適切な手段である場合に限る。
1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

(a) 治安。
(a) public security;

(b) 犯罪の抑止、捜査、検挙、および起訴。
(b) the prevention, investigation, detection and prosecution of criminal offences;

(c) EU または加盟国におけるその他の公共の利益。特に、通貨、予算、課税に関する問題および市場の安定性及び統合性の保護のような EU または加盟国の重要な経済的または財政的な利益。

(c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;

(d) 規制を受ける職業における倫理違反の防止、調査、検出、および起訴。
(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(e) 頻度は少ないとしても、(a)、(b)、(c)、および(d)に規定する場合における職権の行使に伴う監視、点検、または規制の機能。
(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);

(f) データの対象者または他者の権利と自由の保護。
(f) the protection of the data subject or the rights and freedoms of others.

2. 特に、第 1 項での規定に基づいて行うすべての法的措置では、少なくともその処理及び管理者の決定が追求する目的について、具体的な条項を含まなければならない。
2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.

第 IV 章　管理者と処理者
CHAPTER IV CONTROLLER AND PROCESSOR

第 1 節　一般的義務
SECTION 1 GENERAL OBLIGATIONS

第 22 条　管理者の責任
Article 22 Responsibility of the controller

1. 管理者は、個人データの処理がこの規則に準拠して確実に実行されるための方針を定め、かつ適切な対策を講じなければならない。
1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. 第 1 項で規定する対策には、特に以下を含まなければならない。
2. The measures provided for in paragraph 1 shall in particular include:

(a) 第 28 条の規定に基づく文書の保存。

(a) keeping the documentation pursuant to Article 28;

(b) 第 30 条に定められたデータ機密保護要件の実行。
(b) implementing the data security requirements laid down in Article 30;

(c) 第 33 条の規定に基づくデータ保護影響評価の実施。
(c) performing a data protection impact assessment pursuant to Article 33;

(d) 第 34 条(1)(2)の規定に基づく監督機関の事前承諾または事前協議における必要条件の遵守。
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(e) 第 35 条(1)の規定に基づく DPO の任命。
(e) designating a data protection officer pursuant to Article 35(1).

3. 管理者は、第 1 項および第 2 項の規定に基づき講じる対策の有効性を確実に検証できるメカニズムを確立させなければならない。もし適切な場合、独立した内部または外部の監査人にこの検証を行わせなければならない。
3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

4. 委員会には、第 2 項にすでに規定されているものを除き、第 1 項に規定する適切な対策についての評価基準及び必要条件を具体化するため、第 3 項に規定する検証及び監査のメカニズムの条件並びに監査の実施が求められる基準を具体化するため、及び零細、中小規模事業者向けの特段の対策を配慮するため、第 86 条の規定に基づき委任法令を制定する権限が与えられる。
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

第 23 条　設計による初期設定のデータ保護
Article 23 Data protection by design and by default

1. 管理者は、処理の方法を決定するとき及び処理を実施するときの両方において、その処理によりこの規則の必要条件が満たされデータの対象者の権利が確実に保護されるよう、最新技術や実装コストを考慮して、技術的及び組織的な対策と手順を実行しなければなら

ない。
1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. 管理者は、データ量およびデータ保管期間の両方の側面において、特定の処理目的のために必要な個人データだけが処理されその目的に必要な分以上のデータを収集または保持しないことが、初期設定により確保できるメカニズムを確立させなければならない。特にそのメカニズムでは、初期設定により、不特定数の個人が個人データにアクセスできないようにしなければならない。
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. 委員会には、第 1 項及び第 2 項に規定する適切な対策とメカニズム、特に業界、製品、サービスを横断して適用できる設計段階でのデータ保護の評価基準及び必要条件を、より具体的に示すために、第 86 条の規定に基づき、委任法令を制定する権限が与えられる。
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

4. 委員会は、第 1 項および第 2 項に規定する必要条件を満たすための技術標準を定めてもよい。それに関する施行法は、第 87 条(2) に規定する審議手順によって制定されなければならない。
4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 24 条　共同管理者
Article 24 Joint controllers

ある管理者が他者と共同して個人データの処理の目的、条件、および手段を決定する場合は、その管理者同士で協議し、データの対象者が権利を行使するための手順とメカニズムについては特に留意し、この規則における義務を遵守する上での各々の責任を定めなければならない。

Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

第 25 条　EU に拠点を持たない管理者の代理
Article 25 Representatives of controllers not established in the Union

1. 第 3 条(2)に該当する場合、管理者は EU における代理を任命しなければならない。
1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

2. 前項の義務は以下の場合には適用されない。
2. This obligation shall not apply to:

(a) 第 41 条によって十分な水準の保護を実施していると委員会が決定した第三国に拠点を持つ管理者。
(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

(b) 従業員が 250 人未満の事業者。
(b) an enterprise employing fewer than 250 persons; or

(c) 公的機関または公共団体。
(c) a public authority or body; or

(d) EU に在住するデータの対象者に商品やサービスを単に時々提供するだけの管理者。
(d) a controller offering only occasionally goods or services to data subjects residing in the Union.

3. 代理は、商品やサービスの提供と関連して個人データが処理されるまたはその行動が監視されるデータの対象者が居住する加盟国の一つに拠点を持たなければならない。
The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.

4. 管理者による代理の任命は、管理者自身に対する訴訟の提起を妨げるものではない。
The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

第 26 条　処理者
Article 26 **Processor**

1. 管理者の代わりに処理操作が実施される場合、その管理者は、技術的に適正で組織的な対策と手続きを実行することについて十分に保証できる処理者を選出しなければならない。この場合その処理は、この規則の条件を満たし、特にその処理を扱う技術的な安全対策および組織的対策の点でデータの対象者の権利を確実に保護し、そしてこれらの対策に確実に適合していなければならない。
1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. 処理者による処理の実施は、特に処理者が以下を遵守するよう規定して、その処理者を管理者に拘束した契約または他の法的行為によって管理処理者による処理の実施は、処理者を管理者に結びつける契約またはその他の法的行為によって管理されなければならない。そして、その契約や法的行為では、特に下記を規定しなければならない。
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

(a) 処理者は、特に使用する個人データの移転が禁止されている場合、管理者の指示のみに基づき行動すること。
(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

(b) 処理者は、機密を漏らさないと約束した職員または法定の秘密保持義務を負う職員のみを雇用すること。
(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) 処理者は、第 30 条に従ったすべての必要な対策を実施すること。
(c) take all required measures pursuant to Article 30;

(d) 処理者が別の処理者に協力を求める場合、必ず事前に管理者の許可を得ること。
(d) enlist another processor only with the prior permission of the controller;

(e) 処理者は、その処理の本質を考慮して可能な場合には、管理者が第 III 章に定められたデータの対象者の権利を行使する要求に応じる義務の履行に関して、管理者（の意向）に一致する技術的かつ組織的に必要な要件を作成することができるよう、管理者に合意して

技術的および組織的な条件を設定すること。
(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III;

(f) 処理者は、管理者が第 30 条～第 34 条の義務を確実に履行することにおいて管理者を援助することができるよう補助すること。
(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) 処理者は、処理の終了後すべての結果を管理者に引き渡し、個人データを処理しないこと。個人データの処理を中止すること。
(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;

(h) 処理者は、管理者と監督機関に、この条項に定められた義務の履行を管理するために必要なすべての情報を開示すること。
(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.

3. 管理者と処理者は、第 2 項で示された管理者の指示と処理者の義務を文書に記録しなければならない。
3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. 処理者が管理者の指示にはない方法で個人データを処理した場合、その処理者はその処理行為の点において管理者であるとみなされ、第 24 条に定められた共同管理者規則の対象とならなければならない。
4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

5. 第 1 項における処理者の責任、義務、および職務の基準と必要条件、および特に管理と報告の目的において事業グループ内の個人データ処理を容易にするような条件を具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられなければならない。
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

第 27 条　管理者と処理者の権限下での処理
Article 27 Processing under the authority of the controller and processor

個人データを入手できる処理者または管理者の権限下で行動している処理者およびすべての人物は、EU 法または加盟国法でそうすることが求められていない限り、管理者からの指示がなければそれらを処理してはならない。
The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.

第 28 条　文書
Article 28 **Documentation**

1. 各管理者、各処理者、およびもし存在すれば管理者代理は、すべての処理操作に関する文書を責任を持って管理しなければならない。
1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

2. その文書には、少なくとも以下のような情報が含めなければならない。
2. The documentation shall contain at least the following information:

(a) 管理者、または共同管理者か共同処理者の名前と連絡先の詳細。なお、もしある場合、代理の名前と連絡先の詳細。
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;

(b) もし存在するのなら、データ保護職員の名前と連絡先の詳細。
(b) the name and contact details of the data protection officer, if any;

(c) 処理の目的。ここにはその処理が第 6 条(1)(f)に基づくのであれば、管理者が追求する正当な利益が含まれる。
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

(d) データの対象者のカテゴリーとそれらに関連する個人データのカテゴリーに関する記述。
(d) a description of categories of data subjects and of the categories of personal data relating to them;

(e) 正当な利益のために個人データが開示される管理者追求する正当な利益のために個人データが開示される先の管理者を含む、個人データの受取人または受取人のカテゴリー。

(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;

(f) 適切な場合、第三国または国際機関の身元情報を含む第三国または国際機関へのデータ移転。また、第 44 条(1)(h)で言及された移転の場合、適切な予防的手段に関する文書。
(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

(g) 異なるカテゴリーのデータを削除する期限に関する一般的な表示。
(g) a general indication of the time limits for erasure of the different categories of data;

(h) 第 22 条(3)に示されるメカニズムの記述。
(h) the description of the mechanisms referred to in Article 22(3).

3. 管理者、処理者、もし存在すれば管理者代理は、要求があれば監督機関にその文書を開示しなければならない。
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

4. 第 1 項と第 2 項で示された義務は、以下のような管理者と処理者には適用してはならない。
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:

(a) 商業的な利益を得ることなく個人データを処理している自然人。
(a) a natural person processing personal data without a commercial interest; or

(b) 主要業務に付随した活動としてのみ個人データを処理している、従業員が 250 人未満の事業または組織。
(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

5. 特に管理者、処理者、およびもし存在すれば管理者代理の責任を考慮に入れ、第 1 項に示された文書に関する基準と要件をより具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられなければならない。
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

6. 委員会は第 1 項で言及された文書に関する標準形式を定めてもよい。それに関する施行法は、第 87 条(2)に示された試験手順によって採択されなければならない。
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination

procedure referred to in Article 87(2).

第 29 条　監督機関への協力
Article 29 Co-operation with the supervisory authority

1. 管理者、処理者、およびもし存在すれば管理者代理は、特に第 53 条(2)(a)に示された情報の提供および同項(b)で言及されたアクセスの付与のような任務の実施において、要求があれば監督機関に協力しなければならない。
1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. 第 53 条(2)による監督機関の権限の行使に対して、管理者と処理者は、その監督機関が指定した期間内に監督機関に回答をしなければならない。その回答では、監督機関の見解に対して、実施した対策とその結果に関する説明が含まなければならない。
2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

第 2 節　データのセキュリティ
SECTION 2 DATA SECURITY

第 30 条　処理のセキュリティ
Article 30 Security of processing

1. 管理者と処理者は、その最先端技術や実装コストを考慮して、保護する個人データの性質および処理におけるリスクに対して適切なレベルのセキュリティを確保するための技術的および組織的な対策を実施しなければならない。
1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

2. 管理者と処理者は、リスクを評価した後、偶然または不法な破壊あるいは偶然の損失か

ら個人データを保護するために、また、特に個人データの無許可の開示、普及またはアクセス、あるいは改ざんといった不法な処理を防ぐために、第 1 項に示された対策を実施しなければならない。
2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

3. 第 4 項が適用されない場合には、特に初期設定によるデータ保護および設計によるプライバシーの技術やソリューションの動向を考慮に入れ、特定分野における特定のデータ処理の状況での技術水準を明確化し、第 1 項および第 2 項で示された技術的および組織的な手段に関する基準と条件をより具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられなければならない。
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.

4. 委員会は、さまざまな状況、特に以下の目的のために第 1 項および第 2 項で定められた要件を規定する施行法を、必要に応じて採択することができる。
4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:

(a) 個人データへの権限のないアクセスを防ぐため。
(a) prevent any unauthorised access to personal data;

(b) 個人データの権限のない開示、読み込み、コピー、変更、削除、または廃棄を防ぐため。
(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;

(c) 処理操作の合法性を確実に検証するため。
それに関する施行法は、第 87 条(2)に示された試験手順によって採択される。
(c) ensure the verification of the lawfulness of processing operations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 31 条　個人データの侵害に関する監督機関への通知
Article 31 Notification of a personal data breach to the supervisory authority

1. 個人データの侵害が発生した場合、管理者は、それに気が付いてから遅延無く可能なら

24 時間以内に、その個人データの侵害を監督機関に通知しなければならない。24 時間以内に通知しない場合には、それができない合理的な理由も監督機関に通知しなければならない。
1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.

2. 第 26 条(2)(f)により、処理者は個人データの侵害が発生した場合には即時管理者に警告と通知をしなければならない。
2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

3. 第 1 項で示される通知には、少なくとも以下が含まれていなければならない。
3. The notification referred to in paragraph 1 must at least:

(a) その個人データの侵害の性質に関する説明。関係するデータの対象者の数およびカテゴリー、関係するデータレコードの数およびカテゴリーなど。
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) より詳しい情報が入手可能なデータ保護職員、またはその他の問い合わせ先の身元情報と詳しい連絡先。
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;

(c) その個人データの侵害により起こりえる悪影響を軽減するための推薦策。
(c) recommend measures to mitigate the possible adverse effects of the personal data breach;

(d) その個人データの侵害が引き起こす結果。
(d) describe the consequences of the personal data breach;

(e) その個人データの侵害に対処するために管理者が提案または実施した対策。
(e) describe the measures proposed or taken by the controller to address the personal data breach.

4. 管理者は、その個人データの侵害が起こった状況、その影響、および実施した救済・改善策など、個人データの侵害に関するすべての情報を文書に残さなければならない。その文書は、監督機関がこの条項への準拠を検証できるものでなければならない。その文書には、少なくともその目的のために必要な情報が含まれていなければならない。
4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. 第 1 項および第 2 項で示された個人データの侵害の発生、および管理者と処理者がその個人データの侵害を通知しなければならない特定の状況に関する基準と要件をより具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられなければならない。

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. 監督機関への通知のための標準書式、通知の要件に適用される手続き、そこに含まれる情報を削除する期限など第 4 項で示される文書の形式および様式などについて、委員会が定めることができる。それに関する施行法は、第 87 条(2)に示された試験手順によって採択されなければならない。

6.The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 32 条　個人データの侵害に関するデータの対象者への通知

Article 32 Communication of a personal data breach to the data subject

1. 個人情報保護またはデータの対象者のプライバシーに悪影響がありそうな場合、管理者は、第 31 条に示された通知後、遅延なくデータの対象者に、個人データの侵害について通知しなければならない。

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

2. 第 1 項で示されたデータの対象者への通知では、その個人データの侵害の性質について説明し、少なくとも第 31 条(3)(b)および(c)に示される情報と推薦の内容を含められていなければならない。

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).

3. 管理者が、監督機関の満足に至るところまで、実施した適切な技術的保護対策と、それら対策が個人データの侵害に関係するデータに適用されたことを説明したら、データの対象者に、個人データの侵害を通知することは必要としないことにしなくてはならない。その技術的保護対策は、データにアクセスすることが許可されない人物にはデータが理解不

能なものでなければならない。
3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such echnological protection measures shall render the data unintelligible to any person who is not authorised to access it.

4. 個人データの侵害をデータの対象者に通知する管理者義務を果たさないというわけではないにしても、その管理者がまだ通知を行っていない場合には、監督機関はその侵害により考えられる悪影響を考慮してその管理者に通知を行わせることができる。
4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

5. 第 1 項に示された個人データの侵害が個人データに悪影響を与えそうな状況に関する基準と要件をより具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられなければならない。
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.

6. 委員会は、第 1 項に示されたデータの対象者への通知の形式およびその通知の適切な手順を定めることができる。それに関する施行法は、第 87 条(2)に示された審査手順によって採択されなければならない。
6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 3 節　データ保護への影響評価および事前の認可
SECTION 3 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

第 33 条　データ保護への影響評価
Article 33 Data protection impact assessment

1. 処理操作がその性質、適用範囲、または目的によってデータの対象者の権利や自由に特定のリスクを与える場合、管理者またはその管理者の代わりの処理者は、個人データ保護

に対して考えられる処理操作の影響評価を実施しなければならない。
1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. 特に以下のような処理操作は、第 1 項に示される特定のリスクを与えるものである。
2. The following processing operations in particular present specific risks referred to in paragraph 1:

(a) 自動処理に基づき、または個人に関する法的効果を生み出したり、個人に重大な影響を与えたりする手段に基づき、特に自然人の経済的状況、位置、健康、個人的嗜好、信頼性、または行動を分析あるいは予測し、自然人に関する個人的側面を系統的かつ広範囲に評価すること。
(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;

(b) 性生活、健康、人種、および種族的出身に関する情報、または保健医療の提供、疫学的研究、または精神的あるいは感染性の病気の調査のための情報対策の実施または特定の個人に関する決定を行うための大規模なデータ処理。
(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

(c) 誰でも立ち入ることができる地域の監視。特に、光学電子機器(ビデオ監視)を大規模に使用している場合。
(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;

(d) 子供、遺伝データ、またはバイオメトリックデータに関する大規模なファイリングシステムにおける個人データ。
(d) personal data in large scale filing systems on children, genetic data or biometric data;

(e) 第 34 条(2)(b)により監督機関との協議が必要なその他の処理操作。
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).

3. データの対象者および他の関係者の権利と正当な利益を考慮に入れて、その評価には少なくとも、考えられる処理操作の概説、データの対象者の自由と権利に対するリスクの評価、そのリスクへの対策、予防的手段、安全対策、個人情報を確実に保護し、この規則への遵守を実践する仕組みについて示されなければならない。
3. The assessment shall contain at least a general description of the envisaged processing

operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

4. 管理者は、商業的または公的な利益の保護、あるいは、その処理操作のセキュリティには影響を与えない方法により、意図している処理に関してデータの対象者やその代理に意見を求めるものとする。
4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

5. 管理者が公的機関または公的団体であり、処理操作に関することで、また EU 法で規制されるところの規則と手順を示す規則と手順を示す第 6 条(1)(c)による法的義務からその処理が実施された場合には、加盟国が処理活動の前にそのような評価を行うことを必要と思わないのであれば、第 1 項～第 4 項は適用してはならない。
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. スケーラビリティ、検証および監査能力を含め、第 1 項および第 2 項で示された特定のリスクを与えそうな処理操作のための基準と条件、ならびに、第 3 項で示された評価のための要件をより具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられる。その際、委員会は、零細および中小事業のための具体策を検討しなければならない。
6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

7. 委員会は、第 3 項で示された評価を実施、検証、および監査するための基準と手順を明記してもよい。それに関する施行法は、第 87 条(2)に示された試験手順によって採択されなければならない。
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 34 条　事前の認可と事前の協議
Article 34 Prior authorisation and prior consultation

1. 管理者または処理者が第 42 条(2)(d)に示される契約条項を採用、または個人データの第三国または国際機関への移転について第 42 条(5)で示される法的拘束力のある文書において適切な予防的手段を規定していない場合、意図された処理をこの規則に確実に遵守させ、また、特にデータ対象者がさらされるリスクを軽減させるために、管理者または場合によっては処理者は、個人データの処理に先立ち、監督機関から認可を受けなければならない。
1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

2. 管理者またはその代わりの処理者は、意図された処理をこの規則に確実に遵守させ、また特にデータの対象者がさらされるリスクを軽減させるために、以下の場合、個人データの処理に先立ち監督機関に助言を求めなければならない。
2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

(a) 第 33 条に示されるデータ保護への影響評価を実施した結果、その処理操作に、その性質、適用範囲、または目的によって大きな特定のリスクがありそうだと分かった場合。
(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

(b) 第 4 項に示されるような、その性質、適用範囲、および／または目的によって、データの対象者の権利と自由に特定のリスクがありそうな処理操作について、監督機関が事前の協議を実施することが必要と思う場合。
(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3. その意図される処理がこの規則に準拠していない、特にリスクについて十分に特定されず、または十分に軽減されていないと監督機関が判断した場合、監督機関はその意図される処理を禁止し不適合を正すための適切な提案をしなければならない。
3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or

mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

4. 監督機関は、第 2 項(b)による事前の協議の対象となった処理操作のリストを作成および公開しなければならない。監督機関はそのリストを欧州データ保護委員会に提供しなければならない。
4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

5. 第 4 項に示されたリストが、複数の加盟国におけるデータの対象者への商品やサービスの提供に関する処理活動を意味する場合、データの対象者の行動を監視する処理活動である場合、またはそのリストが EU 内の個人データの自由な移動に大きな影響を与えかねない処理活動である場合、監督機関はそのリストを採用する前に第 57 条に示された一貫性のある仕組みを適用しなければならない。
5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

6. 管理者または処理者は、第 33 条に示されるデータ保護への影響評価の結果を監督機関に提供しなければならない。また、要求があれば管理者または処理者は監督機関がその処理のコンプライアンス、特にデータの対象者の個人データ保護におけるリスク、および関連する予防的手段を評価することができる、その他の情報も提供しなければならない。
6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7. 意図された処理をこの規則に確実に遵守させ、また、準拠し、特にデータの対象者へのリスクを軽減するために、加盟国は、法的措置を国民議会で採択したり処理の性質を定義したその法的措置に基づく対策を準備したりする場合には、監督機関に助言を求めなければならない。
7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

8. 第 2 項(a)に示された、大きな特定のリスクを決定する基準と要件をより具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられなければならない。
8. The Commission shall be empowered to adopt delegated acts in accordance with Article

86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.

9. 委員会は、第 1 項および第 2 項に示された事前の認可と協議のための標準形式と手順、ならびに第 6 項による監督機関への通知のための標準形式と手順を提示してもよい。それに関する施行法は、第 87 条(2)に示された試験手順によって採択されなければならない。
9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 4 節　データ保護職員
SECTION 4 DATA PROTECTION OFFICER

第 35 条　データ保護職員の指名
Article 35 Designation of the data protection officer

1. 管理者および処理者は、以下の場合には、データ保護職員を指名しなければならない。
1. The controller and the processor shall designate a data protection officer in any case where:

(a) その処理が、公的機関または公共団体によって行われる場合。または
(a) the processing is carried out by a public authority or body; or

(b) その処理が、従業員が 250 人以上の企業によって行われる場合。または
(b) the processing is carried out by an enterprise employing 250 persons or more; or

(c) 管理者または処理者の中心的な業務が、その性質、適用範囲、そして／または目的によって、データの対象者の日常的かつ系統的な監視を必要とする処理操作である場合。
(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

2. 第 1 項(b)の場合、一つの事業グループに一人のデータ保護職員を指名すればよい。
2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

3. 管理者または処理者が公的機関または公共団体の場合、その組織構造を考慮に入れ、いくつかの実体に対して一人のデータ保護職員を任命することもできる。
3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

4. 第 1 項で示されていない場合でも、管理者、処理者、協会、または管理者や処理者のカテゴリーにを表すその他の団体は、データ保護職員を任命してもよい。
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. 管理者または処理者は、プロとしての資質、特にデータ保護法と慣例に関する専門知識および第 37 条に示された業務を遂行する能力に基づいて、データ保護職員を指名する。その専門知識として必要なレベルは、特に実施されるデータ処理および管理者または処理者によって処理される個人データの保護に従って決定されなければならない。
5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

6. 管理者または処理者は、そのデータ保護職員が他の職業における義務も担っている場合には、確実にそれをデータ保護職員としての職務や義務と一致し、利害の衝突が起きないようにしなければならない。
6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

7. 管理者または処理者は、最低でも 2 年間データ保護職員を指名しなければならない。そのデータ保護職員を更なる期間について再指名してもよい。在任期間中、データ保護職員がその義務を果たすための条件を満たせなくなった場合に限り、そのデータ保護職員を解任してもよい。
7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.

8. データ保護職員は、管理者または処理者が雇用してもよいし、請負契約に基づいて職務に就かせてもよい。
8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. 管理者または処理者は、データ保護職員の名前と詳しい連絡先を、監督機関および一般に開示する。
9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

10 データの対象者には、そのデータの対象者のデータ処理、およびこの規則における権利

の行使に関連するすべての問題について、データ保護職員に問い合わせる権利がなければならない。
10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

11. 第 1 項(c)で示された管理者または処理者の中心的な業務の基準と要件、および第 5 項で示されたデータ保護職員のプロとしての資質の基準をより具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられなければならない。
11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

第 36 条　データ保護職員の地位
Article 36 Position of the data protection officer

1. 管理者または処理者は、データ保護職員が確実に個人データ保護に関するすべての問題に適切かつ直ちに関与できるようにしなければならない。
1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. 管理者または処理者は、データ保護職員がその義務と職務を独立して遂行し、その職務の遂行について指示を受けないということを確実にしなければならない。データ保護職員は、管理者または処理者の経営陣に直接報告しなければならない。
2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.

3. 管理者または処理者は、データ保護職員による職務の遂行を補助し、第 37 条に示された義務と職務を遂行するために必要な職員、施設、設備、およびその他の資源を提供しなければならない。
3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

第 37 条　データ保護職員の職務
Article 37 Tasks of the data protection officer

1. 管理者または処理者は、少なくとも以下の職務をデータ保護職員に委託しなければならない。
1. The controller or the processor shall entrust the data protection officer at least with the following tasks:

(a) この規則による管理者または処理者に彼らの義務について通知および勧告すること。また、この活動および受け取った回答を文書化すること。
(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;

(b) 個人データの保護に関して管理者または処理者が設定した方針の実施と適用の監視。責任の割り当て、処理操作にかかわる職員のトレーニング、および関連する監査など。
(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;

(c) 特に、設計によるデータ保護、初期設定によるデータ保護およびデータセキュリティに関する要件、ならびに、データの対象者の情報およびこの規則におけるデータの対象者の権利の行使の要求に関するこの規則の実施および適用を監視すること。
(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;

(d) 第 28 条で示された文書が維持されていることを保証すること。
(d) to ensure that the documentation referred to in Article 28 is maintained;

(e) 第 31 条と第 32 条による、個人データの侵害に関する文書、通知、および連絡を監視すること。
(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

(f) 第 33 条と第 34 条により要求があったら、管理者または処理者によるデータ保護への影響評価の実施、および事前の認可または事前の協議の申請を監視すること。
(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;

(g) 監督機関の要求に対する回答を監視すること。データ保護職員の権限内であれば、監督機関の要求に応じた、またはデータ保護職員自らの決断による監督機関との共同活動を行うこと。
(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory

authority at the latter's request or on the data protection officer’s own initiative;

(h) 処理に関する問題について監督機関の代わりの問い合わせ先となること。適切であれば、データ保護職員自らの決断により監督機関と協議すること。
(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

2. 第 1 項で示されたデータ保護職員の職務、証明、状況、権限、および資源に関する基準と要件をより具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられなければならない。
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.

第 5 節　行動規範と認証
SECTION 5 CODES OF CONDUCT AND CERTIFICATION

第 38 条　行動規範
Article 38 Codes of conduct

1. この規則を適切に運用するために、様々なデータ処理の分野において、特に以下を考慮した行動規範を作成することを、加盟国、監督機関、および委員会は奨励しなくてはならない。
1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

(a) 公正で透明性の高いデータ処理。
(a) fair and transparent data processing;

(b) データの収集。
(b) the collection of data;

(c) 公衆とデータの対象者の情報。
(c) the information of the public and of data subjects;

(d) データの対象者がその権利を行使する要求。
(d) requests of data subjects in exercise of their rights;

(e) 子供の情報と保護。

(e) information and protection of children;

(f) 第三国または国際機関へのデータの転送。
(f) transfer of data to third countries or international organisations;

(g) 管理者がその行動規範を遵守するよう監視およびそれを保証するための仕組み。
(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;

(h) 第 73 条と第 75 条によるデータの対象者の権利を侵害することなく、個人データの処理について管理者とデータの対象者との間に発生した論争を解決するための示談手続き、およびその他の論争の解決手順。
(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. ある加盟国において管理者または処理者のカテゴリーに入る協会およびその他の団体が、行動規範を作成したり既存の行動規範を修正または拡張したりする場合には、それらを同じ加盟国の監督機関に提出して意見を求めてもよい。その監督機関は、行動規範の草稿や修正案がこの規則に準拠しているかどうかについて意見を述べることができる。その監督機関は、データの対象者または彼らの代理に、これらの草案への意見を求めなければならない。
2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

3. 複数の加盟国における管理者のカテゴリーに入る協会およびその他の団体は、行動規範の草稿、および既存の行動規範への修正案または拡張案を、委員会に提出することができる。
3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.

4. 委員会は、第 3 項によって提出された行動規範および既存の行動規範への改正または拡張が、EU において一般的な妥当性を持っているか否かを決定するために、施行法を採択してもよい。それに関する施行法は、第 87 条(2)に示された審査手順によって採択されなければならない。
4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. 委員会は、第 4 項により一般的な妥当性を持っていると決定された行動規範については、適切な公開を確実に行わなくてはならない。
5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

第 39 条　認証
Article 39 Certification

1. 加盟国と委員会は、特に欧州規模でデータ保護を認証する仕組みを構築し、データ保護シールおよびマークを作成し、データの対象者が管理者と処理者が提供するデータ保護のレベルを簡単に評価できるようにすることを奨励する。そのデータ保護の認証の仕組みは、様々な分野における異なる処理操作の特徴をふまえ、この規則の適切な運用に寄与しなくてはならない。
1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

2. 第 1 項で示されたデータ保護認証の仕組みの評価基準と必要条件、例えばその付与と取り消しに関する条件や EU や第三国での認知のための必要条件をより具体的に示すために、第 86 条に従って委任決議を採択する権限が委員会に与えられなければならない。
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.

3. データ保護認証の仕組み、シール、およびマークを普及させ認知してもらうために、委員会はそのための技術規格を定めてもよい。それに関する施行法は、第 87 条(2)に示された審査手順によって採択されなければならない。
3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

第 V 章　第三国または国際機関への個人データの転送
CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

第 40 条　転送における一般原則
Article 40 General principle for transfers

個人データを処理してから第三国または国際機関に転送したり、または転送後に処理をする予定でそれらを転送したりすることは、管理者と処理者が、この規則の他の条項と併せてこの章が定める条件に準拠した場合に限り認められる。その転送には、ある第三国または国際機関からまた別の第三国または国際機関に個人データを再転送することも含まれる。
Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

第 41 条　妥当性を評価した上での転送
Article 41 Transfers with an adequacy decision

1. 転送は、問題となる第三国または第三国の領土や処理部門、国際機関については、委員会が、適正な水準の個人データ保護を行っていると決定した場合に限り行ってもよい。このような転送においては、追加的な認可は不要とする。
1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.

2. 保護レベルの妥当性を評価するとき、委員会は、以下のような要素を考慮しなくてはならない。
2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

(a) その国または国際機関が準拠する治安、国防、国家安全、刑法、職業規則、そして安全対策などに関する一般的な、または分野別の有効な法の支配と法律。また、データの対象者、特に EU 在住の個人データが転送されるデータの対象者のための、有効な行政上および法的な救済のような効果的で法的強制力のある権利。
(a) the rule of law, relevant legislation in force, both general and sectoral, including

concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

(b) データ保護規則への準拠、データの対象者による自らの権利の行使に対する補助および助言、および EU や加盟国の監督機関との協力に責任を持つ一つ以上の独立した監督機関が問題となる第三国または国際機関に存在し、効果的に機能しているということ。
(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) 問題となる第三国または国際機関が実施している国際的な関与。
(c) the international commitments the third country or international organisation in question has entered into.

3. 委員会は、第 2 項で示される意味の範囲によって、第三国、その第三国の領土あるいは処理部門、または国際機関が、適正な水準の個人データ保護をきちんと行っているということを決定できる。それに関する施行法は、第 87 条(2)に示された審査手順によって採択される。
3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

4. 施行法では地理的かつ分野別の適用を規定し、適切であれば第 2 項(b)で言及された監督機関が特定されていなければならない。
4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.

5. 特に、第三国または国際機関における一般的な、または分野別の有効な法律が、データの対象者、特に EU 在住で個人データが転送されるデータ対象者のための、有効な行政上および法的な救済のような効果的で法的強制力のある権利を保証していない場合には、委員会は、第 2 項で示される意味の範囲において、第三国または第三国の領土や処理部門、国際機関については、適正な水準の個人データ保護を行っていないということを決定してもよい。それに関する施行法は、第 87 条(2)に示された審査手順によって採択される。または、個人のデータ保護に関する権利について緊急性の高い場合には、第 87 条(3)に示された手順によって採択されなくてはならない。
5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where

the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).

6. 委員会が第 5 項の決定を下した場合、問題となる第三国または第三国の領土や処理部門、国際機関への個人データの転送は、第 42 条～第 44 条にこだわることなく、すべて禁止される。委員会は、適切な時期にその第三国または国際機関と第 5 項の決定により定められた状況を是正する観点から協議を開始する。
6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.

7. 委員会は、適正な水準の個人データ保護が実施されている、または実施されていないということを決定した際、その第三国、その第三国の領土あるいは処理セクター、または国際機関のリストを『*Official Journal of the European Union*（EU 官報）』に公開しなければならない。
7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.

8. 委員会が指令 95/46/EC 第 25 条(6)または第 26 条(4)に基づき採用した決定事項は、それが委員会により修正、差し替え、または廃止されない限り、引き続き有効である。
8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.

第 42 条　適切な安全対策を介した転送
Article 42 Transfers by way of appropriate safeguards

1. 委員会が第 41 条による決定を下していない場合は、管理者または処理者は、法的拘束力のある手段で個人情報保護に関する適切な安全対策を提示した場合に限り、第三国あるいは国際機関に個人データを転送することができる。
1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only

if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

2. 第 1 項に言及される適切な安全対策には、特に以下の事項を規定しなくてはならない。
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

(a) 第 43 条に従った拘束的企業準則。
(a) binding corporate rules in accordance with Article 43; or

(b) 委員会が採用した標準データ保護条項。それに関する施行法は、第 87 条(2)に示された審査手順によって採択されなくてはならない。
(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or

(c) 第 57 条に示された整合性機構により監督機関が採用した標準データ保護条項。ただし、第 62 条(1)(b)により委員会が一般に妥当だと宣言した場合に限る。
(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or

(d) 第 4 項により監督機関が認可した、管理者または処理者とデータの受取人との間に交わされた契約条項。
(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

3. 第 2 項(a)、(b)、または(c)に言及される標準データ保護条項あるいは拘束的企業準則に基づく転送については、追加的な認可は不要である。
3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.

4. 第 2 項(d)に言及される契約条項に基づく転送を実施する場合、管理者または処理者は、第 34 条(1)(a)によりその契約条項について監督機関から事前の認可を受けなければならない。その転送が、他の加盟国におけるデータの対象者にかかわる処理活動、または EU 内の個人データの自由な移動に著しい影響を与えるような処理活動に関係している場合には、監督機関は第 57 条に示された一貫性のある仕組みを適用しなければならない。
4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5. 個人情報保護に関する適切な安全対策が法的拘束力のある手段で場合には、管理者また

は処理者は、その転送、または一連の転送、またはその転送の根拠を示す行政上の取り決めに加えられる条項について、事前の認可を受けなければならない。その監督機関による認可は、第 34 条(1)(a)に基づくものとする。その転送が、他の加盟国におけるデータの対象者にかかわる処理活動、または EU 内の個人データの自由な移動に著しい影響を与えるような処理活動に関係している場合には、監督機関は第 57 条に示された一貫性のある仕組みを適用しなければならない。監督機関が指令 95/46/EC 第 26 条(2)に基づき与えた認可は、それがその監督機関により修正、差し替え、または廃止されない限り、引き続き有効である。

5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.

第 43 条　拘束的企業準則による転送

Article 43 Transfers by way of binding corporate rules

1. 監督機関は、第 58 条の一貫性のある仕組みに基づく拘束的企業準則を承認する。ただし、以下のような場合に限る。

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:

(a) 法的な拘束力があり、管理者または処理者の事業グループのすべてのメンバー、及びその従業者に適用され、実施される。

(a) are legally binding and apply to and are enforced by every member within the controller’s or processor's group of undertakings, and include their employees;

(b) その拘束的企業準則は、データの対象者に強制的に執行できる権利を明示的に与えている。

(b) expressly confer enforceable rights on data subjects;

(c) その拘束的企業準則は、第 2 項に定められた必要条件を満たしている。

(c) fulfil the requirements laid down in paragraph 2.

2. 拘束的企業準則には、少なくとも以下を明記しなくてはならない。

2. The binding corporate rules shall at least specify:

(a) 事業グループとそのメンバーの体制と詳しい連絡先。
(a) the structure and contact details of the group of undertakings and its members;

(b) 個人データのカテゴリー、処理の種類とその目的、影響を受けるデータ主体の種別、および問題となる第三国もしくは複数の第三国の識別を含むデータの転送、もしくは一連の転送。
(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) 規則の国内及び国外における法的拘束性。
(c) their legally binding nature, both internally and externally;

(d) 特に目的の制限、データの品質、処理に関する法的根拠、機微な個人データについての、一般的なデータ保護の原則。データセキュリティを確実にするための措置。政策により拘束されない組織に再転送する際の必要条件。
(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;

(e) 第 20 条によるプロファイリングに基づく手段の対象とはならない権利、第 75 条による管轄監督機関および加盟国管轄裁判所に苦情を申し立てる権利、および拘束的企業準則の侵害に関する救済、適切な場合には補償を受ける権利のような、データの対象者の権利およびそれらの権利を行使する手段。
(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) EU に拠点を持たない事業グループのメンバーによってその拘束的企業準則が侵害された場合には、加盟国の領土に拠点を持つ管理者または処理者が責任を負うことへの承諾。その管理者または処理者は、損害を引き起こした出来事についてそのメンバーには責任がないということを立証できた場合に限り、上記の責任の全体または一部が免除される。
(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;

(g) その拘束的企業準則、特に本項(d)、(e)、および(f)に言及される条項に関する情報が、第 11 条によりデータの対象者に提供される方法。

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;

(h) 第 35 条に従って任命されたデータ保護職員の職務。事業グループにおける拘束的企業準則への準拠の監視、トレーニングおよび苦情処理の監視など。
(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;

(i) 事業グループにおける拘束的企業準則への準拠を検証する仕組み。
(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;

(j) 方針の変更を報告および記録し、それらの変更を監督機関に報告するための仕組み。
(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;

(k) 特に本項(i)に言及された手段の検証結果を監督機関に開示することによる、事業グループ内の全メンバーのコンプライアンスを保証するためのその監督機関との協力の仕組み。
(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.

3. 委員会には、本条項の意味での拘束的企業準則に関する評価基準と必要条件、特にそれらの承認の評価基準、処理者が準拠する拘束的企業準則への第 2 項(b)、(d)、(e)、および(f)の適用、そしてデータの対象者の個人データ保護を保証するためのさらなる必要条件をより具体的に示すために、第 86 条に従って委任決議を採択する権限が与えられなければならない。
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.

4. 委員会は、本条項の意味での拘束的企業準則について、管理者、処理者、そして監督機関の間における電子手段による情報交換の形式と手順を指定してもよい。それに関する施行法は、第 87 条(2)に示された審査手順によって採択される。
4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

第 44 条　逸脱
Article 44 Derogations

1. 第 41 条に準拠した妥当性の決定が下されていない場合または第 42 条に準拠した適切な安全対策が欠如している場合、以下のいずれかを満たしている場合に限り、第三国または国際機関への個人データの転送または一連の転送が認められる。
1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(a) 妥当性の決定及び適切な安全対策がないことによる転送のリスクがあらかじめ通知され、データの対象者が提案された転送に同意した場合。
(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or

(b) データの対象者と管理者との間における契約の履行のため、またはデータの対象者の要求により事前に契約上の措置を実施するため、その転送が必要な場合。
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) 管理者とデータの対象者以外の自然人または法人との間において、データの対象者の利益のため行われる契約の締結または履行のために、その転送が必要な場合。
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) 公共の利益を実現するための重要な理由に基づきその転送が必要な場合。
(d) the transfer is necessary for important grounds of public interest; or

(e) 法的請求の成立、行使または弁明のために、その転送が必要な場合。
(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(f) データの対象者が物理的または法的に同意を与えることができない場合において、そのデータの対象者または別の人物の重大な利益を保護するためにその転送が必要な場合。
(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or

(g) EU 法または加盟国法が定める特定の場合における協議条件が満たされている範囲で、EU 法または加盟国法に基づき公に情報提供が行われており、一般大衆もしくは正当な利益を実証できる任意の人による公開協議が可能な登録簿によって、その転送が行われる場合。
(g) the transfer is made from a register which according to Union or Member State law is

intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) 発生頻度が高い、または規模が大きいものではなく、管理者または処理者がそのデータ転送または一連のデータ転送の操作に関するすべての状況を評価し必要に応じ個人情報保護のための適切な安全対策を提示している場合に限り、管理者または処理者が追求する正当な利益のための転送が必要である場合。
(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

2. 第 1 項(g)による転送は、その登録簿における個人データ全体または個人データの全カテゴリーを含めてはならない。その登録簿において正当な権益をもつ人々が協議を行う場合は、それらの人々からの要求があった場合またはそれらの人々自体が受取人になる場合に限りその転送が実施される。
2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. 第 1 項(h)に基づき処理を実施する場合、管理者または処理者は、そのデータの性質、提案される処理操作または一連の処理操作の目的および期間、加えて発信国、第三国、および最終目的国の状況、必要であれば個人データ保護のための適切な安全対策に関して、特に考慮をしなければならない。
3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.

4. 第 1 項(b)、(c)、および(h)は、公的機関がその権限の行使において行う活動には適用してはならない。
4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. 第 1 項(d)で言及される公共の利益は、管理者を対象とする EU 法または加盟国法において認識されなければならない。
5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.

6. 管理者または処理者は、第 1 項(h)で言及される評価および適切な安全対策を、第 28 条

で言及される文書に記録して、監督機関にその転送について通知しなければならない。
6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.

7. 委員会には、第 1 項(d) で意味する範囲で「公共の利益を実現するための重要な理由」の特定、第 1 項(h)で言及される適切な安全対策の評価基準や必要条件を規定する目的において、第 86 条に従って委任決議を採択する権限が与えられなければならない。
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.

第 45 条　個人データ保護のための国際協力
Article 45 International co-operation for the protection of personal data

1. 第三国および国際機関に対して、委員会および監督機関は、以下を実現するために適切な措置を講じなければならない。
1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) 個人データ保護に関する法律の施行を促進するために、有効な国際協力のための仕組みの展開。
(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;

(b) 個人データの保護およびその他の基本的人権と自由のための適切な安全対策を条件として、通知、苦情照会、調査支援、および情報交換を含む個人データ保護の法律の施行における国際的な相互扶助の提供。
(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) 個人データ保護に関する法律の施行における国際協力の促進を目的とした議論と活動の、適切な利害関係者への関与。
(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) 個人データ保護に関する法律および慣例の取り交わしと文書化の促進。

(d) promote the exchange and documentation of personal data protection legislation and practice.

2. 第 1 項の内容を実現するために、委員会は、それが第 41 条(3)の意味における適正水準の保護を実施しているとした第三国または国際機関および特にそれらの監督機関との関係を深めて行くために、適切な措置を講じなければならない。
2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).

第 VI 章　独立監督機関
CHAPTER VI INDEPENDENT SUPERVISORY AUTHORITIES

第 1 節　独立の状態
SECTION 1 INDEPENDENT STATUS

第 46 条　監督機関
Article 46 Supervisory authority

1. 自然人の個人データの処理において彼らの基本的権利と自由を保障し、EU 域内における個人データの自由な流通を促進するために、各加盟国は、一つ以上の公的機関がこの規則の運用の監視および EU 域内を通した一貫性のある適用に責任を持つよう定めなければならない。この目的のために、監督機関は相互に協力し、委員会にも協力するものとする。
1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission.

2. ある加盟国において二つ以上の監督機関が設立された場合、その加盟国は一つの監督機関を指定するものとし、欧州データ保護委員会当局が効果的に関与できる唯一の連絡先として機能させる。そして、第 57 条の一貫性のある仕組みに関するルールにより、他の監督機関とのコンプライアンスが確保されるような仕組みを構築するものとする。
2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with

the rules relating to the consistency mechanism referred to in Article 57.

3. 各加盟国は、本章に従って採択した法の条項について、遅くとも第 91 条(2)で指定された期日までに委員会に通知する。後日それらに影響を与える修正条項を作成した場合には、遅延無く委員会に通知する。
3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

第 47 条　独立
Article 47 Independence

1. 監督機関は、委任された職務権限を行使する際、完全に独立して行動しなければならない。
1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.

2. 監督機関のメンバーは、その職務の実施において、誰にも指示を求めず、誰からも指示を受けないものとする。
2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.

3. 監督機関のメンバーはその義務に反する一切の行動を控え、在任期間中には、それが有利であるか否かに関係なく、その義務に反することになる職業には一切従事してはならない。
3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. 監督機関のメンバーは、任期の終了後に就任を受諾したり便益を受け取ったりする場合には、誠実に思慮深く行動しなくてはならない。
4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.

5. 各加盟国は、その監督機関の職務権限、または欧州データ保護委員会との相互扶助、協力、および参加に関する職務権限を効果的に行使するために必要な、人的、技術的、および財政的資源、施設、インフラが、確実に監督機関に提供されるようにしなくてはならない。
5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in

the context of mutual assistance, co-operation and participation in the European Data Protection Board.

6. 各加盟国は、その監督機関が、機関の代表により任命されその指示に従うような機関独自の職員を確実に持つようにする。
6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.

7. 加盟国は、監督機関が財務管理を受ける際にはその独立性には影響がないということを保証しなくてはならない。加盟国は、監督機関には別枠の年度予算を与えなくてはならない。またその予算は開示されなくてはならない。
7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.

第 48 条　監督機関のメンバーに関する一般条件
Article 48 General conditions for the members of the supervisory authority

1. 加盟国は、監督機関のメンバーがその加盟国の議会または政府によって任命されるよう定めなくてはならない。
1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.

2. 監督機関のメンバーは、その独立性には疑う余地が無く、個人データ保護の分野において確実に義務を果たすために必要な経験と技能を持っている人々から選出されなくてはならない。
2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.

3. 監督機関のメンバーの職務は、第 5 項に従って、任期満了、辞職、または定年退職により終了するものとする。
3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.

4. 監督機関のメンバーがその義務を果たすための条件をもはや満たしていない場合、または重大な過失により有罪となった場合には、管轄している国家の法的処置によりそのメンバーを解雇、または年金その他の福利厚生を受ける権利を剥奪することができる。
4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.

5. メンバーが辞職またはその任期が満了した場合でも、新しいメンバーが任命されるまでは引き続きその職務を実施しなくてはならない。
5. Where the term of office expires or the member resigns, the member shall continue to exercise the duties until a new member is appointed.

第 49 条　監督機関の設立に関する規則
Article 49 Rules on the establishment of the supervisory authority

各加盟国は、この規則の範囲内で、以下を法律により定めるものとする。
Each Member State shall provide by law within the limits of this Regulation:

(a) 監督機関の設立とその地位。
(a) the establishment and status of the supervisory authority;

(b) 監督機関のメンバーの義務を果たすために必要な資格、経験、および技能。
(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;

(c) 監督機関のメンバーを任命するための規則と手順、および監督機関の職務に反する行動または職業に関する規則。
(c) the rules and procedures for the appointment of the members of the supervisory authority, as well the rules on actions or occupations incompatible with the duties of the office;

(d) 監督機関のメンバーの任期。任期は 4 年以上とする。ただし、この規則の発効から最初の任命において、その手続きをずらすことが監督機関の独立性を保つために必要ならば、4 年より短くてもよい。
(d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) 監督機関のメンバーに再任を認めるかどうか。
(e) whether the members of the supervisory authority shall be eligible for reappointment;

(f) 監督機関のメンバーおよびスタッフの職務義務を適用する規則と一般条件。
(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;

(g) 監督機関のメンバーがその義務を果たすための条件をもはや満たしていない場合、または重大な過失により有罪となった場合における、監督機関のメンバーの職務の終了に関するルールと手順。

(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including in case that they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.

第 50 条　職業上の守秘義務
Article 50 Professional secrecy

監督機関のメンバーおよびスタッフは、その任期中または退任後を問わず、公務の実施において知ったすべての機密情報について職業上の守秘義務を負わなくてはならない。
The members and the staff of the supervisory authority shall be subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.

第 2 節　義務と権限
SECTION 2 DUTIES AND POWERS

第 51 条　管轄
Article 51 Competence

1. 各監督機関は、それが属する加盟国の領土において、この規則によって付与された権限を行使しなくてはならない。
1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.

2. その個人データの処理が EU 域内の管理者または処理者の拠点において実施され、その管理者または処理者が二カ国以上の加盟国に拠点を持っている場合には、本規則の第 VII 章の条項に従い、その管理者または処理者の主要拠点における監督機関が全加盟国におけるそれらの処理活動を管轄しなくてはならない。
2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.

3. 監督機関は、法廷がその司法権力により行う処理操作は監督しないものとする。
The supervisory authority shall not be competent to supervise processing operations of

courts acting in their judicial capacity.

第 52 条　義務
Article 52 Duties

1. 監督機関は以下を実施しなくてはならない。
1. The supervisory authority shall:

(a) この規則の適用の監視および保証。
(a) monitor and ensure the application of this Regulation;

(b) 第 73 条に従ってデータの対象者またはその対象者の代理の協会によるあらゆる苦情の申し立てに対応し、その苦情に関する調査を適切な範囲で実施し、そして、特に別の監督機関との調査や調整が必要な場合には妥当な期間内に、そのデータの対象者または協会に苦情処理の進捗状況と結果を報告する。
(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(c) 他の監督機関と情報を共有し相互扶助を行う。また、この規則の適用と実施における一貫性を確保する。
(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;

(d) 調査は、自発的に、または苦情を受けたり他の監督機関から要求されたりした場合に実施する。そして、データの対象者がその監督機関に苦情を申し立てていた場合には、妥当な期間内にそのデータの対象者に調査結果を報告する。
(d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period;

(e) 個人データの保護に影響を与えるような動向を監視する。特に、情報通信技術と商習慣における動向を監視する。
(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(f) 個人データの処理において個人の権利と自由を守るための立法上および行政上の手段について、加盟国の組織や団体から相談を受ける。

(f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

(g) 第 34 条で言及された処理操作を認可し、それに関する相談を受ける。
(g) authorise and be consulted on the processing operations referred to in Article 34;

(h) 第 38 条(2)による行動規範の草稿への意見を表明する。
(h) issue an opinion on the draft codes of conduct pursuant to Article 38(2);

(i) 第 43 条に従って、拘束的企業準則を承認する。
(i) approve binding corporate rules pursuant to Article 43;

(j) 欧州データ保護委員会の活動に参加する。
(j) participate in the activities of the European Data Protection Board.

2. 各監督機関は、個人データの処理に関するリスク、ルール、予防的手段、および権利について一般の認識を高めるようにする。子供向けの活動については特に配慮するものとする。
2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.

3. 監督機関は、データの対象者からの要求があれば、彼らがこの規則により権利を行使する際に助言を与えなくてはならない。そして適切な場合には、その目的のために他の加盟国の監督機関とも協力しなくてはならない。
3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

4. 第 1 項(b)で言及された苦情の申し立てについて、監督機関は苦情を申し立てるための様式を提供しなくてはならない。その様式は電子形式とするが、それ以外の通信手段も排除しない。
4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.

5. 監督機関によるデータの対象者のための職務の実施は、無料としなくてはならない。
5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.

6. その要求が明らかに度を越えている場合、特に反復して行われる場合には、監督機関は料金を請求してもよいし、またはデータの対象者に要求された対応を行わなくてもよい。その場合、監督機関は、その要求が明らかに度を越えているということについて立証責任を負わなくてはならない。
6. Where requests are manifestly excessive, in particular due to their repetitive character,

the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.

第 53 条　権限
Article 53 Powers

1. 各監督機関には、以下のような権限を持たなくてはならない。
1. Each supervisory authority shall have the power:

(a) 個人データ処理条項の侵害の疑いについて、管理者または処理者に通知する。適切な場合には、その管理者または処理者に具体的な方法によるその侵害の改善を命令し、データの対象者の保護を行う。
(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;

(b) この規則に基づく権利を行使するデータの対象者の要求に応じるよう、管理者または処理者に命令する。
(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;

(c) 管理者、処理者、および適切な場合その代理に対して、監督機関の義務を果たすために必要なあらゆる情報を提供するように命令する。
(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;

(d) 第 34 条による事前の認可と事前の協議への準拠を確保する。
(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;

(e) 管理者または処理者を注意または訓戒する。
(e) to warn or admonish the controller or the processor;

(f) この規則の条項に違反して処理されたすべてのデータの修正、削除、もしくは、破壊を命じる。また、そのデータが開示された第三者に同様のことを行うように通知を出すよう命じる。
(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;

(g) 個人データの処理を一時的または決定的に禁止する。

(g) to impose a temporary or definitive ban on processing;

(h) 第三国または国際機関における受取人へのデータの送信を保留する。
(h) to suspend data flows to a recipient in a third country or to an international organisation;

(i) 個人データの保護に関するすべての問題について意見を表明する。
(i) to issue opinions on any issue related to the protection of personal data;

(j) 個人データの保護に関するすべての問題について、国民議会、政府、他の政治機関、および一般大衆に通知する。
(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.

2. 各監督機関は、管理者または処理者から以下を得ることができる調査権限を持たなくてはならない。
2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:

(a) 監督機関の義務を果たすために必要なあらゆる個人データおよび情報へのアクセス。
(a) access to all personal data and to all information necessary for the performance of its duties;

(b) この規則に違反した活動が行われていると推定できる合理的な根拠がある場合には、その施設への立ち入り、およびあらゆるデータ処理機器や媒体へのアクセス。
上記(b)で言及される権限は、EU 法および加盟国法に準拠して行使されなければならない。
(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.

The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.

3. 各監督機関は、特に第 74 条(4)と第 75 条(2)により、この規則への違反を司法機関に通知し法的措置を取る権限を持たなくてはならない。
3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).

4. 各監督機関は、特に第 79 条(4)、(5)、および(6)で言及されるような行政上の違反に対し制裁を加える権限を持たなくてはならない。
4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).

第 54 条　活動報告
Article 54 Activity report

各監督機関は、その活動に関する年次報告書を作成しなければならない。その報告書は国民議会に提出され、一般大衆、委員会、および欧州データ保護委員会にも開示されなくてはならない。
Each supervisory authority must draw up an annual report on its activities. The report shall be presented to the national parliament and shall be made be available to the public, the Commission and the European Data Protection Board.

第 VII 章　連携と一貫性
CHAPTER VII CO-OPERATION AND CONSISTENCY

第 1 節　連携
SECTION 1 CO-OPERATION

第 55 条 相互支援
Article 55 Mutual assistance

1. 監督機関は本規則を一貫した姿勢で施行および適用するため、関連情報の相互提供と相互支援を行うべきとし、効果的に連携するための措置を他方と共同で整備しなければならない。相互支援に特に必要となる情報請求や監督措置には、事前の認可と事前の協議の要請、調査、及び、調査開始に際しての速やかな通知等を含まなくてはならない。また、処理業務によって複数加盟国におけるデータ対象者に影響が生じる可能性がある場合にはその後の進捗状況について把握しなくてはならない。
1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data subjects in several Member States are likely to be affected by processing operations.

2. 各監督機関は他方の監督機関からの請求に対し、請求の受領から遅滞なく返信する上で必要な全ての適切な措置を取るものとし、その期間は 1 ヶ月を超えないものとする。この措置には特に、調査実施にあたっての関連情報の送信、または本規則に反した処理業務を停止もしくは禁止させるための強制措置などが含まれる。

2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.

3. 支援要請には、要請の目的や要請理由等、必要な全情報を含むものとする。取り交わされた情報は、要請された案件に関してのみに使われるべきである。
3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.

4. 支援要請を受けた監督機関は、以下の場合を除きその要請に従うことを断ってはならない。
4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:

(a) 当該機関がその要請に対する管轄権を有さない場合、もしくは
(a) it is not competent for the request; or

(b) 要請の順守によって本規則の規定に抵触する可能性がある場合
(b) compliance with the request would be incompatible with the provisions of this Regulation.

5. 要請を受けた監督機関は、他方の監督機関に対し、その結果もしくは状況に応じ、当該機関から受けた要請の遂行にあたり実施した措置の進捗状況を通知しなくてはならない。
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.

6. 監督機関は、他の監督機関から請求された情報を、標準化フォーマットを用い、電子的手段によってできるだけ速やかに提供するべきものとする。
6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.

7. 相互支援の要請を受けて行ういかなる対応に対しても、費用を請求してはならない。
7. No fee shall be charged for any action taken following a request for mutual assistance.

8. 監督機関が他方の監督機関からの請求より 1 ヶ月のうちに対応しなかった場合、請求した監督機関は第 51 条(1)に従い、当該加盟国領内にて暫定措置を取り、第 57 条の手順に従って欧州データ保護委員会に本件を委ねるものとする。
8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.

9. 当該監督機関はその暫定措置の有効期間を明示すべきものとする。この期間は 3 ヶ月を超えてはならない。当該監督機関はその措置について、十分な理由を添えて、遅滞なく欧州データ保護委員会および欧州委員会に連絡すべきものとする。
9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.

10. 欧州委員会は本条で述べる相互支援の手順とフォーマット、および、監督機関同士または監督機関と欧州データ保護委員会との間で電子的手段にて情報を交換する際の手続き、具体的には第 6 項に述べる標準化フォーマットを定めることができる。これらの実施にかかる布告は、第 87 条(2)の審査手順に従って採択されるべきものとする。
10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

第 56 条 監督機関の共同運用
Article 56 Joint operations of supervisory authorities

1.連携と相互支援促進のため、監督機関は、他の加盟国における監督機関から指定されたメンバーもしくはスタッフと共に、共同で調査任務、強制措置、その他の作業を執り行うべきものとする。
1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved.

2. 複数加盟国に渡るデータの対象者が処理業務によって影響を受ける可能性がある場合、これら加盟国の各監督機関は必要に応じ、共同調査任務または共同作業に参加する権利を有する。管轄権を有する監督機関は、これら加盟国の各監督機関を適切な共同調査任務または共同作業に参加させるべく招聘し、これら作業に参加を求める監督機関に遅滞なく対応するべきものとする。
2. In cases where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without

delay.

3. 各監督機関は主催監督機関として、国内法に則り、補佐監督機関の認可を受けた上で、共同調査任務に関わる補佐監督機関のメンバーもしくはスタッフへ調査任務を含む執行権を付与する、あるいは、主催監督機関の国内法の範囲で、補佐監督機関のメンバーもしくはスタッフに、補佐監督機関の国内法に基づいた執行権行使の許可を与えるものとする。かかる執行権は、ルールにより主催監督機関のメンバーもしくはスタッフの立会いが必要であり、その指導に基づいてのみ行使が可能である。補佐監督機関のメンバーもしくはスタッフは、主催監督機関における国内法を順守しなくてはならないが、その行動の責任は主催監督機関が負うものとする。

3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their executive powers in accordance with the seconding supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.

4. 監督機関は特定の連携活動の履行について策定すべきとする。

4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions.

5. 監督機関が第 2 項に定める義務を 1 ヶ月以内に順守しない場合、他の監督機関が第 51 条(1)に従って当該加盟国の領内における暫定措置を取るものとする。

5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1).

6. 監督機関は第 5 項に定める暫定措置の有効期間を明示すべきものとする。この期間は 3 ヶ月を超えてはならない。当該監督機関はその措置について、十分な理由と共に、遅滞なく欧州データ保護委員会および欧州委員会に連絡すべきものとし、第 57 条における一貫性のある仕組みに事態を届け出るものとする。

6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.

第 2 節　一貫性
SECTION 2 CONSISTENCY

第 57 条 一貫性のある仕組み
Article 57 Consistency mechanism

第 46 条(1)に定める目的のため、各機関および欧州委員会は本節に定める一貫性のある仕組みを通じて互いに協力すべきものとする。
For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism as set out in this section.

第 58 条 欧州データ保護委員会による見解
Article 58 Opinion by the European Data Protection Board

1. 監督機関が第 2 項の措置を採択する前に、当該監督機関は欧州データ保護委員会および欧州委員会に対策案を通知しなければならない。
1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

2. 第 1 項に定める義務は、法的効力の発生を意図した以下に関する措置に対して適用されるべきものである。
2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:

(a) 複数加盟国のデータの対象者への物品やサービスの提供に関するもの、もしくは対象者の行動を監視するデータ処理活動に関するもの、または
(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or

(b) EU 域内での個人データの自由な移動に多大な影響を与える可能性があるもの、または
(b) may substantially affect the free movement of personal data within the Union; or

(c) 第 34 条(5)に従って、事前協議の対象となる処理業務の一覧の採択を目指すもの、または
(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or

(d) 第 42 条(2)(c)の標準データ保護条項の決定を目指すもの、または

(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or

(e) 第 42 条(2)(d)の契約条項の認可を目指すもの、または
(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or

(f) 第 43 条の意義の範囲で拘束的企業準則の承認を目指すもの。
(f) aims to approve binding corporate rules within the meaning of Article 43.

3. 監督機関または欧州データ保護委員会は、特に監督機関が第 2 項の対策案を提出しない場合、もしくは第 55 条に準じた相互支援または第 56 条の共同業務に対する義務を順守しない場合に、その事象を一貫性のある仕組みにおいて対応するよう求めることができる。
3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

4. 本規則を正確かつ一貫して確実に適用するため、欧州委員会は一貫性のある仕組みを用いて事態に対処するよう求めることができる。
4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.

5. 監督機関および欧州委員会は、これらの措置に関する事実の要旨、対策案および根拠等に関する連絡を、必要に応じ、標準化フォーマットを用い、電子的手段によって連絡すべきものとする。
5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.

6. 欧州データ保護委員会の委員長は標準化フォーマットを用い、自分に伝えられた全ての関連情報を、欧州データ保護委員会の構成員および欧州委員会に対し、即座に電子的手段を用いて通知するべきものとする。委員長は必要に応じ、それらに関する情報の翻訳を提供しなくてはならない。
6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.

7. 欧州データ保護委員会は、構成員の過半数による採決があった場合、もしくは第 5 項に基づく関連情報を受領してから 1 週間の内に監督機関もしくは欧州委員会から要請を受けた場合に、当該案件に対する見解を公表するものとする。その見解については、欧州データ保護委員会構成員の過半数による採決により 1 ヶ月以内に採択されるべきものとする。

委員長は状況に応じ、第 1 項および第 3 項の監督機関と欧州委員会および第 51 条における管轄監督機関に対し、妥当な期間内にその見解を通知し公表すべきものとする。
7.The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.

8. 第 1 項の監督機関および第 51 条における管轄権を有する監督機関は、欧州データ保護委員会の見解を考慮に入れ、欧州データ保護委員会の委員長よりの見解の情報が出されてから 2 週間の内に、当該機関が対策案の維持もしくは改定を行うか否か、また改定後の対策案がある場合にはそれを、標準化フォーマットを用い、電子的手段によって欧州データ保護委員会の委員長および欧州委員会に対し、通知すべきとする。
8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

第 59 条 欧州委員会による見解
Article 59 Opinion by the Commission

1. 本規則を正確かつ一貫して確実に適用させるため、第 58 条に基づいて事態が提起されてより 10 週間以内、もしくは最長でも第 61 条の事例から 6 週間以内に、欧州委員会は第 58 条もしくは第 61 条に基づいて提起された事態への見解を採択することができる。
1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.

2. 第 1 項に従って欧州委員会が見解を採択した場合、かかる監督機関は欧州委員会の見解を最大限に考慮し、対策案の維持もしくは改定の意図を欧州委員会および欧州データ保護委員会に対して通知しなければならない。
2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission’s opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.

3. 第 1 項の期間は、監督機関は対策案を採択してはならない。
3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.

4. 当該監督機関が欧州委員会の見解に意図的に従わない場合、当該機関は欧州委員会および欧州データ保護委員会に対し、第 1 項の期間内に通知を行い、その理由を提示するべきものとする。この場合、更に 1 か月の間は対策案を採択することはできない。
4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.

第 60 条 対策案の延長
Article 60 Suspension of a draft measure

1. 第 59 条(4)の連絡がなされてから 1 ヶ月以内に、対策案によって本規則が正確かつ確実に適用されるかについて、もしくはその対策案によって本規則が誤用される可能性について、欧州委員会が深刻な疑いを抱いている場合には、第 58 条(7)および第 61 条(2)に沿って以下を成す上で必要との観点から欧州データ保護委員会が発行した見解を考慮に入れ、当該監督機関に対策案の採択を延期するよう求める適切な決議を採択することができる。
箇条 59(4)の通知後 1 ヶ月以内に、対策案によってこの規則が確実に正しく適用されるか、又は正しく適用されず、結果として一貫性のない適用となるかどうかについて、欧州委員会が深刻な疑念をもつ場合で、下記のことを行うために必要と思われる場合には、欧州委員会は、第 58 条(7)及び第 61 条(2)に従って欧州データ保護委員会が発行した見解を考慮し、監督機関が対策案の採択を保留するように求める、合理的な決定を採択してよい。
1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:

(a) もしまだ可能と思われる場合には、監督機関および欧州データ保護委員会における見解の一致を図る、または
(a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or

(b) 第 62 条(1)(a)号に準じて措置を採択する。
(b) adopt a measure pursuant to point (a) of Article 62(1).

2. 欧州委員会は保留期間を定めねばならず、その期間は 12 ヶ月を超えてはならない。
The Commission shall specify the duration of the suspension which shall not exceed 12 months.

3. 第 2 項の期間は、監督機関は対策案を採択することはできない。
During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.

第 61 条 緊急時の手順
Article 61 Urgency procedure

1. 例外的な事例として、監督機関がデータの対象者の利益を保護する上で急を要する対応が必要だと見なす場合、特にデータの対象者の現在の状況が変わることで権利行使が大きく妨げられる場合、または多大な不利益を回避するため、もしくはそれ以外の理由等の場合に、第 58 条の手順から逸脱した手段を用い、監督機関は特定の期間のみ有効な保全措置をただちに採択することができる。当該監督機関はこれらの措置について、全ての理由を添え、欧州データ保護委員会および欧州委員会に対して遅滞なく連絡すべきものとする。
監督機関がデータの対象者の利益を守るために緊急の対応が必要と考える場合、特に既存の状況の変更によってデータの対象者の利益の行使が著しく妨げられる危険があるような例外的状況においては、多大な不利益を回避するため、又は他の理由で、箇条 58 の手順からの逸脱により、監督機関はある特定の期間のみ有効な暫定措置を直ちに採択してよい。監督機関はこれらの措置について、十分な理由を添えて遅滞なく欧州データ保護委員会及び欧州委員会に通知しなければならない。
1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.

2. 監督機関が第 1 項に従った措置を取り、その後最終措置の採択が至急必要だと考える場合、最終措置の緊急性の理由を含め、欧州データ保護委員会の見解が至急必要である理由を提示し、その緊急時見解を求めることができる。
2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.

3. データの対象者の利益を守るために緊急の対応が必要な状況下において管轄権を有する監督機関が適切な措置を取らなかった場合、監督機関は迅速な対応が必要な理由等、欧州データ保護委員会の見解が至急必要である理由を提示し、その緊急時見解を求めることができる。
3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.

4. 第 58 条(7)の規定によらない本条第 2 項および第 3 項の緊急時見解は、欧州データ保護委員会の構成員の単純多数による採決から 2 週間以内に採択されるものとする。
4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.

第 62 条 実施法行為
Article 62 Implementing acts

1. 欧州委員会は以下の目的で実施法行為を採択することができる。
1. The Commission may adopt implementing acts for:

(a) 第 60 条(1)に従って適切な決議が採択されたという事態、もしくは監督機関が対策案を提出せず、第 59 条に従って採択された欧州委員会の見解に従う意図がない旨を当該機関が示したという事態について、第 58 条もしくは第 61 条に沿った監督機関からの連絡を受けて、本規則の目的と要件に沿った正確な適用を決定するため
(a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;

(b)第 58 条(2)(d)の標準データ保護条項案を一般的妥当性をもつものとして公表するかについて、第 59 条(1)の期間内に決定するため
(b) deciding, within the period referred to in Article 59(1), whether it declares draft standard data protection clauses referred to in point (d) of Article 58(2), as having general validity;

(c) 本節で定める整合性機構の適用のためのフォーマットと手順を特定するため
(c) specifying the format and procedures for the application of the consistency mechanism referred to in this section;

(d) 監督機関間および監督機関と欧州データ保護委員会との間で電子的手段にて情報を交

換する際の取決め、特に第 58 条(5)、(6)および(8)の標準フォーマットを策定するため
これらの実施法行為は、第 87 条(2)の審査手順に従って採択されなければならない。
(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

2. 第 1 項(a)号の事例におけるデータの対象者の利益に関し、やむを得ない緊急性を示す正当な根拠がある場合、欧州委員会は第 87 条(3)の手順に従って迅速に適切な実施法行為を採択すべきものとする。これらの法は 12 ヶ月を超えない範囲で有効に存続するものとする。
2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.

3. 本節における措置の欠如もしくは採択は、欧州委員会が条約に基づいて採択したその他の措置を毀損するものではない。
3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.

第 63 条 執行
Article 63 Enforcement

1. 本規則において、一加盟国の監督機関による法的に執行可能な措置は、関連する全ての加盟国において執行されるべきものとする。
1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.

2. 監督機関が第 58 条(1)から(5)に違反して整合性機構に対策案を提出しなかった場合、当該監督機関の措置は法的に有効かつ執行可能とはならない。
2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.

第 3 節　欧州データ保護委員会
SECTION 3 EUROPEAN DATA PROTECTION BOARD

第 64 条 欧州データ保護委員会
Article 64 European Data Protection Board

1. 本規則によって欧州データ保護委員会を設立する。
1. A European Data Protection Board is hereby set up.

2. 欧州データ保護委員会は、各加盟国から選出された 1 監督機関の長と、欧州データ保護監督者で構成されるものとする。
2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.

3. 本規則に基づく規定適用の監督に際し、ある加盟国において 2 つ以上の監督機関が担当する場合、それら機関のうち 1 つの機関の長を、共同代表者として任命するものとする。
3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.

4. 欧州委員会は欧州データ保護委員会の活動および会議に参加する権利を有すべきものとし、代表者を指定するものとする。欧州データ保護委員会の委員長は、欧州データ保護委員会の全活動について遅延なく欧州委員会に通知すべきものとする。
4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.

第 65 条 独立性
Article 65 Independence

1. 欧州データ保護委員会は第 66 条および第 67 条に沿ってその業務を遂行する際には、独立的に行動すべきものとする。
1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67.

2. 欧州データ保護委員会は、第 66 条第 1 項(b)号および第 2 項の欧州委員会による要求を毀損することなく、自らの任務を遂行する際、他者の指示を求めたり、その指示に従ったりしてはならない。
2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.

第 66 条 欧州データ保護委員会のタスク
Article 66 Tasks of the European Data Protection Board

1. 欧州データ保護委員会は、本規則の一貫した適用を確実なものとするものとする。この趣旨の下、欧州データ保護委員会は自らの主導もしくは欧州委員会からの要請にて、特に以下を成すべきものとする。
1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:

(a) 連合内の個人データの保護におけるあらゆる課題に対して欧州委員会に助言を行う。その課題には、本規則に対する改定提案等が含まれる。
(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(b) 自発的に、メンバーからの要請で、もしくは欧州委員会からの要請にて、本規則の適用に纏わる疑問を精査し、本規則の一貫した適用を促進するために、監督機関に対してガイドライン、提言、および最良事例を公表する。
(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;

(c) (b)号のガイドライン、提言、および最良事例の実際的な適用を評価し、これらについて定期的に欧州委員会に報告する。
(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;

(d) 第 57 条の整合性機構に従い、監督機関の決定案に対して見解を述べる。
(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;

(e) 監督機関間の、二者間もしくは複数機関間の協力並びに効果的な情報および実務例の交換を推進する。
(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;

(f) 監督機関間の、また適切な場合には第三国もしくは国際機関との、共通の訓練計画を推進し人材交流を促進する。
(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

(g) 世界中のデータ保護監督機関との間の、データ保護に関する法律や実務例に関する知識及び文書の交換を推進する。
(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

2. 欧州委員会が欧州データ保護委員会からの助言を求める場合、その事例の緊急性を検討した上で、その助言に回答期限を定めることができる。
2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.

3. 欧州データ保護委員会は欧州委員会および第 87 条の委員会に対し、自らの見解、ガイドライン、提言、および最良事例を送付し、公開すべきものとする。
3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.

4. 欧州委員会は、欧州データ保護委員会により出された見解、ガイドライン、提言、および最良事例に基づいて取った対応を、欧州データ保護委員会に通知するものとする。
4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

第 67 条 報告
Article 67 Reports

1. 欧州データ保護委員会は定期的かつ適時に、欧州委員会に対し自らの活動結果を報告するものとする。欧州連合および第三国における、自然人の保護および個人データの処理に関する状況についての年次報告書を策定するべきものとする。その報告書には、第 66 条(1)(c)号のガイドライン、提言、および最良事例の実用的な適用に関する報告を含むものとする。
1. The European Data Protection Board shall regularly and timely inform the Commission about the outcome of its activities. It shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries. The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).

2. 報告は公開の上、欧州議会、欧州理事会および欧州委員会に伝達されるものとする。
2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.

第 68 条 手順
Article 68 Procedure

1. 欧州データ保護委員会はその構成員の単純多数によって議事を決するものとする。
1. The European Data Protection Board shall take decisions by a simple majority of its members.

2. 欧州データ保護委員会は手順に関する独自の規則を採択し、自らの運用協定を編成するものとする。特に、構成員の任期が切れた場合、もしくは構成員が辞任した場合の職務継続的遂行、特定の課題またはセクターに関するサブグループの設立、および第 57 条の整合性機構に関連する手順を提供するものとする。
2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.

第 69 条 委員長
Article 69 Chair

1. 欧州データ保護委員会は構成員の中から委員長 1 名および副委員長 2 名を選出するものとする。副委員長のうち 1 名は、委員長に選任されていない限り、欧州データ保護監督者でなければならない。
1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members. One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair.

2. 委員長および副委員長の任期は 5 年とし、更新可能とする。
2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable.

第 70 条 委員長の職務
Article 70 Tasks of the chair

1. 委員長は以下の職務を負うものとする。

1. The chair shall have the following tasks:

(a) 欧州データ保護委員会会議を招集し、議題を準備する。
(a) to convene the meetings of the European Data Protection Board and prepare its agenda;

(b) 欧州データ保護委員会の職務、特に第 57 条の整合性機構に関する職務を、確実に適時に履行する。
(b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.

2. 欧州データ保護委員会は、委員長および副委員長の職権について委員会手順に関する規則の中で定めるものとする。
2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.

第 71 条 事務局
Article 71 Secretariat

1. 欧州データ保護委員会は事務局を有するものとする。欧州データ保護監督者がその事務局を提供するものとする。
1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat.

2. 事務局は委員長の指示の下、欧州データ保護委員会に分析的、運営管理的および後方業務的な支援を提供するものとする。
2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair.

3. 事務局は、特に以下について責任を負うものとする。
3. The secretariat shall be responsible in particular for:

(a) 欧州データ保護委員会の日々の業務
(a) the day-to-day business of the European Data Protection Board;

(b) 欧州データ保護委員会の構成員、同委員長および欧州委員会間の連絡、および他機関や公共に向けての連絡
(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;

(c) 内部および外部との連絡における電子的手段の利用
(c) the use of electronic means for the internal and external communication;

(d) 関連情報の翻訳

(d) the translation of relevant information;

(e) 欧州データ保護委員会の会議準備およびフォローアップ;
(e) the preparation and follow-up of the meetings of the European Data Protection Board;

(f) 欧州データ保護委員会が採択した見解およびその他文書の準備、立案ならびに発行
(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.

第 72 条 守秘義務
Article 72 Confidentiality

1. 欧州データ保護委員会での議論は機密とする。
1. The discussions of the European Data Protection Board shall be confidential.

2. 欧州データ保護委員会の構成員、専門家、および第三者機関の代表により提出された文書は、欧州委員会規則(EC) No 1049/2001 に基づいて開示許可が与えられるか、もしくは欧州データ保護委員会が一般に公開しない限り、機密とする。
2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.

3. 欧州データ保護委員会の構成員の構成員に加え、専門家および第三者機関の代表は、本条に定める守秘義務を順守するよう求められる。委員長は、専門家および第三者機関の代表者に、自らに課せられた守秘義務要件について確実に認知させなければならない。
3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.

第 VIII 章　救済、法的責任および制裁措置
CHAPTER VIII REMEDIES, LIABILITY AND SANCTIONS

第 73 条 監督機関への不服申し立ての権利
Article 73 Right to lodge a complaint with a supervisory authority

1. 各データの対象者は、自らに関する個人データの処理が本規則に準じていないと考える

場合、行政または司法救済を毀損することなく、加盟国の監督機関に対して不服を申し立てる権利を有するものとする。
1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.

2. 個人データの保護に関するデータの対象者の権利と利益を保護することを目指し、加盟国の法律に準じて適切に構成された団体、機関もしくは組合は、個人データの処理によって本規則におけるデータの対象者の権利が侵害されたと考える場合、1 名以上のデータの対象者の代表として、当該加盟国の監督機関に対して不服を申し立てる権利を有するものとする。
2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.

3. 第 2 項の団体、機関もしくは組合は、個人データの侵害が生じたと考える場合には、データの対象者の不服とは別に、当該加盟国の監督機関に対して不服を申し立てる権利を有するものとする。
3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.

第 74 条 監督機関に対して司法救済を求める権利
Article 74 Right to a judicial remedy against a supervisory authority

1. 各自然人もしくは法人は、自らに関してなされた監督機関の決定に対し、司法救済を求める権利を有するものとする。
1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.

2. 各データの対象者は、自らの権利を保護する上で必要な決定がなされない、もしくは第 52 条(1)(b)号における不服に対する進捗状況または結果が 3 ヶ月以内にデータの対象者に通知されていないとの不服に基づいて、監督機関に対応を義務付ける司法救済を求める権利を有するものとする。
2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on

the progress or outcome of the complaint pursuant to point (b) of Article 52(1).

3. 監督機関に対する訴訟は、監督機関が存在する加盟国の裁判所に提起されるものとする。
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. 自らが居住する国ではなく、他の加盟国の監督機関の決定に影響を受けるデータの対象者は、当該案件への管轄権を有する他加盟国の監督機関に対して自らの代理として訴訟手続きを取るよう、自らの住む加盟国の監督機関に求めることができる。
4. A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.

5. 加盟国は本条における裁判所による最終判決を履行するものとする。
5. The Member States shall enforce final decisions by the courts referred to in this Article.

第 75 条 管理者もしくは処理者に対して司法救済を求める権利
Article 75 Right to a judicial remedy against a controller or processor

1. 第 73 条の監督機関への不服申し立ての権利を含むあらゆる行政救済を毀損することなく、各自然人は、本規則に準じない個人データの処理によって本規則に基づく自らの権利が侵害されたと考える場合、司法救済を求める権利を有するものとする。
1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

2. 管理者または処理者に対する訴訟は、管理者もしくは処理者が施設を有する加盟国にて提起されるべきものとする。管理者が公権力を行使する公的機関である場合を除き、当該訴訟をデータの対象者が住まう加盟国にて提起しても良い。
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.

3. 同様の措置、決定または実施に関する訴訟が第 58 条の整合性機構においても係争中である場合、データの対象者の権利を保護する上で、整合性機構の手順の結果を待つことができないほど緊急の場合を除き、裁判所は訴訟を保留することができる。

3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.

4. 加盟国は本条における裁判所による最終判決を履行するものとする。
4. The Member States shall enforce final decisions by the courts referred to in this Article.

第 76 条 訴訟手続の共通規則
Article 76 Common rules for court proceedings

1. 第 73 条(2)の団体、機関もしくは組合は、1 名以上のデータの対象者の代理として第 74、75 条の権利を行使する権利を有するものとする。
1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.

2. 各監督機関は、本規則における規定の履行、もしくは連合内における個人データ保護の確実な整合のために、法的手続きを取り訴訟を起こす権利を有するものとする。
2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.

3. 加盟国にて管轄を有する裁判所が、他加盟国において並行訴訟が提起されていると信じる相当な理由がある場合、当該裁判所は当該加盟国の担当裁判所に連絡を取り、並行訴訟の有無について確認すべきものとする。
3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.

4. 他方の加盟国にて同様の措置、決定または実施に関わる並行訴訟がなされている場合、裁判所は当該訴訟を保留することができる。
4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.

5. 加盟国は、経過措置、あらゆる被疑侵害の処分を行うよう策定された措置、および係る利益の更なる損害を防ぐ措置等を国内法の元で迅速に採択するための訴訟を起こす手段を、確実に整備する必要がある。
加盟国は、侵害の申立てを終結させ、これに関与する利益の更なる損害を防ぐための、暫定処置を含めた措置の迅速な採択が、国内法の下で可能な訴訟によって確実に行われるよ

うにしなければならない。
5. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

第 77 条 賠償を受ける権利と法的責任
Article 77 Right to compensation and liability

1. 違法な処理操作もしくは本規則に適合しない活動の結果により損害を受けた者は、受けた損害に対し、管理者もしくは当該被害を引き起こした処理者から賠償を受ける権利を有するものとする。
1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.

2. 当該処理に 2 人以上の管理者もしくは処理者が関与する場合、各管理者もしくは処理者は被害総額に対する連帯責任を負うものとする。
2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.

3. 管理者もしくは処理者がその損害を引き起こした事象に対して責任がないことを証明する場合、同者はその一部もしくは全ての法的責任を免れる。
3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.

第 78 条 罰則
Article 78 Penalties

1. 加盟国は、例えば管理者が代表者を指名する義務に従わなかった等、本規則における条項に違反した場合に適用する罰則を定め、それらが確実に施行されるよう必要な全ての措置を取るものとする。その罰則は効果的、均衡的かつ抑止的でなければならない。
1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.

2. 管理者が代表者を設置している場合、その罰則は代表者に適用されるべきものとなるが、その場合に管理者に対する罰則を毀損することはない。
2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller.

3. 各加盟国は第 1 項に従って同国法に採択したこれら条項について最長でも第 91 条(2)に定める期日までに、そして以後これらに影響を与える改定について遅延なく、欧州委員会に対して通知すべきものとする。
3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

第 79 条 行政的制裁措置
Article 79 Administrative sanctions

1. 各監督機関は本条に従って行政的制裁措置を課す権限を与えられるものとする。
1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.

2. 各事例における行政的制裁措置は、効果的、均衡的かつ抑止的でなければならない。その過料は、違反の性質、重大さおよび期間、違反の性質、自然人もしくは法人による責任の度合い、および過去の違反の有無、第 23 条に従って施行された技術的および組織的措置、ならびに違反の救済にあたっての監査機関との協力の程度に配慮して設定されるべきものとする。
2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.

3. 本規則の不履行が初回であり意図的ではなかった場合、以下の場合には書面による警告のみとし、制裁を科さなくともよい。
3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:

(a) 自然人が個人データを商業的関心なく処理した場合、または
(a) a natural person is processing personal data without a commercial interest; or

(b) 従業員 250 名未満の事業者もしくは組織が、その主要業務の補助としてのみ個人データ

の処理を行った場合
(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.

4. 監督機関は、以下を故意または過失によって行う者に対して最大 250,000 ユーロを、事業者の場合には全世界での年間売上高のうち最大で 0.5%までを過料として科すべきものとする。
4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(a) データの対象者による要請に対応する仕組を提供しない、または第 12 条(1)および(2)に従った迅速な対処もしくは必要なフォーマットによる対応を行わない
(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);

(b) 第 12 条(4)に背き、データの対象者への情報提供もしくは要請への対処のために料金を請求する
(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).

5. 監督機関は、以下を故意または過失によって行う者に対して最大 500,000 ユーロ、もしくは事業者の場合には全世界での年間売上高のうち最大で 1%までを過料として科すべきものとする。
5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(a) データの対象者に対し、第 11 条、第 12 条(3)および第 14 条に準じた情報提供を行わない、もしくは不完全な情報を提供した、または十分な透明性のある方法での情報提供を行わない
(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;

(b) 第 15 条および第 16 条に準じたデータへのアクセスをデータの対象者に提供しない、または個人データの修正を行わない、または受信者に対し、第 13 条に準じた適切な情報の交信を行わない
(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;

(c) 第 17 条に準じた忘れてもらう権利もしくは削除権を遵守しない、または期限を監視する仕組みの確実な導入を行わない、もしくはデータの対象者が個人データのリンク、複写、

複製の削除を要請していることを第三者に通知する必要な手段をとらない
(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;

(d) 第 18 条に違反し、個人データの複写を電子的媒体で提供しない、もしくはデータの対象者が他のアプリケーションに個人データを送信するのを妨害する
(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;

(e) 第 24 条に準じた管理者に対し、各自の責任を策定しない、もしくは不十分な策定を行う
(e) does not or not sufficiently determine the respective responsibilities with cocontrollers pursuant to Article 24;

(f) 第 28 条、第 31 条(4)、および第 44 条(3)に準じた文書を管理しない、もしくは不十分な管理を行う
(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);

(g) 特別分野のデータが関与しない場合に、第 80 条、第 82 条および第 83 条、ならびに表現の自由に関する規則または雇用現場におけるデータ処理規則もしくは歴史的、統計的、および科学的調査目的での処理要件を遵守しない
(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.

6. 監督機関は、以下を故意または過失によって行う者に対して最大 1,000,000 ユーロ、もしくは事業者の場合には全世界での年間売上高のうち最大で 2%までを過料として科すべきものとする。
6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(a) 第 6 条、第 7 条および第 8 条に準じた個人データ処理に関する法的根拠なく、または不十分な状態で、または同意に関する要件を遵守せずにデータを処理する
(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;

(b) 第 9 条および第 81 条に背き、特別分野のデータを処理する
(b) processes special categories of data in violation of Articles 9 and 81;

(c) 第 19 号の異議もしくは要求に従わない
(c) does not comply with an objection or the requirement pursuant to Article 19;

(d) 第 20 条のプロファイリングに基づいた手段に関する要件を遵守しない
(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;

(e) 第 22 条、第 23 条及び第 30 条に準じた内部規約の採択、または確実な法令遵守とその証明を行うための適切な措置の実施を行わない
(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;

(f) 第 25 条による代表者の指名を行わない
(f) does not designate a representative pursuant to Article 25;

(g) 第 26 条および第 27 条にある管理者の代理としての義務に違反した個人データの処理もしくは処理の指示を行う
(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;

(h) 第 31 条および第 32 条に沿った個人データの侵害に対する警告もしくは通知、監督機関もしくはデータ対象者に適時もしくは全くデータ侵害について通知しない
(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;

(i) 第 33 条および第 34 条に準じたデータ保護影響評価を実施しない、または監督機関による事前の認可または事前協議無しに個人データ処理を行う
(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;

(j) 第 35 条、第 36 条および第 37 条にあるデータ保護オフィサーの任命を行わない、もしくはその役割を確実に果たすための条件を実行しない
(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;

(k) 第 39 条のデータ保護シールもしくはマークを誤用する
(k) misuses a data protection seal or mark in the meaning of Article 39;

(l) 第 40 条から第 44 条による妥当性の判断、または適切なセーフガードによって許可されていない、第三者国もしくは国際機関に対し、または当該条項を逸脱してデータ送信を行う、または行うよう指示する
(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;

(m) 第 53 条(1)にある、データ処理またはデータフローの保留に対する監督機関からの命令、もしくは一時的または永久な禁止に従わない

(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);

(n) 第 28 条(3)、第 29 条、第 34 条(6)および第 53 条(2)に定める監督機関に対する補佐、または対応、関連情報の提供、もしくは敷地への立ち入り許可を行わない
(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);

(o) 第 84 条の業務上の守秘義務に関する防護対策の規則を遵守しない
(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.

7. 欧州委員会は、第 2 項の基準を考慮し、第 4 項、第 5 項ならびに第 6 項の過料の額を更新する目的で、第 86 条に従って委任法令を採択する権限を与えられるものとする。
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.

第 IX 章　特定のデータ処理の状況に関する規定
CHAPTER IX PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

第 80 条 個人データの処理と表現の自由
Article 80 Processing of personal data and freedom of expression

1. 加盟国は、第 II 章の一般的原則、第 III 章のデータの対象者の権利、第 IV 章の管理者および処理者の権利、第 V 章の第三者国ならびに国際機関への個人データの送信、第 VI 章の独立監督機関、第 VI 章の監査機関の連携と整合性の条項に対し、表現の自由を定める規則に則り、個人データ保護の権利と調和させるために個人データの処理を報道的な目的、もしくは芸術的、文学的表現で行う場合に対する適用除外および特例を提示すべきものとする。
1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

2. 各加盟国は第 1 項に従って同国法に採択したこれら条項について最長でも第 91 条(2)に定める期日までに、そして以後の改定法またはこれらに影響を与える改定について遅延なく、欧州委員会に対して通知すべきものとする
2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.

第 81 条 個人の健康に関するデータの処理
Article 81 Processing of personal data concerning health

1. 本規則の限度および第 9 条(2)(h)号に従い、個人の健康に関するデータの処理は、データの対象者の利益を保護するために適切かつ具体的な措置を提供する EU 法もしくは加盟国法に基づき、かつ以下のために必要なものでなければならない。
1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:

(a) 対象となるデータが職業上の守秘義務の対象となる医療従事者、もしくは加盟国法もしくは同国内で管轄権を有する組織が策定した規則によって、同等の守秘義務が課せられる者による、予防医学、職業病医学、医療診断、看護と治療の提供、または医療サービス管理の目的で行うデータ処理のため、または
(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or

(b) 公衆衛生の分野における、健康への深刻な越境的脅威に対する保護、もしくは、とりわけ医療機器や医薬品に対する高い品質や安全性基準の保証等の公共の利益のため、または
(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or

(c) 健康保険制度で手当やサービスへの申し立て手順の品質や費用対効果を徹底させる等、社会保護等のその他公共の利益のため
(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.

2. 歴史的、統計的または科学的調査目的に必要な、例えば診断の向上及び類似した病気の

区別化、治療の準備等のために立ち上げた患者台帳等の、個人の健康に関するデータの処理は、第 83 条の条件および保護措置の対象になる。
2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.

3. 欧州委員会は、第 1 項(b)号の公衆衛生分野における公共の利益の他の理由、及び第 1 項の個人データの処理への保護措置に対する基準と要件を更に特定する目的で、第 86 条に従って委任法令を採択する権限を与えられるものとする。
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

第 82 条 職場での処理
Article 82 Processing in the employment context

1. 本規則の範囲で、 加盟国は法律によって、職場での被雇用者の個人データの処理を規制する特定の規則を採択することができる。それらの規則には特に、採用目的、法律や団体協約に定める責務の遂行等を含む雇用関係の遂行、業務の計画および編成、職場での健康と安全等の目的、および雇用に関する権利と利益の個人または集団レベルでの享受および遂行目的、および雇用関係終了の目的のためのものを含む。
1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2.各加盟国は第 1 項に従って同国法に採択したこれら条項について最長でも第 91 条(2)に定める期日までに、そして以後これらに影響を与える改定について遅延なく、欧州委員会に対して通知すべきものとする
2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

3. 欧州委員会は、第 1 項の個人データの処理への保護措置に対する基準と要件を更に特定する目的で、第 86 条に従って委任法令を採択する権限を与えられるものとする。

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

第 83 条 歴史的、統計的、および科学的調査目的での処理
Article 83 Processing for historical, statistical and scientific research purposes

1. 本規則の範囲で、以下の場合においてのみ、個人データは歴史的、統計的および科学的調査目的での処理が許される。
1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:

(a) データの対象者の特定、もしくはこれ以上の特定を許可しない類のデータを処理する以外の方法では、これらの目的が達成できない場合
(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

(b) データの対象者が特定された又は特定が可能な情報の属性が与えられたデータが他の情報とは別に保管されており、その情報を用いることでこれらの目的が達成可能である場合
(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.

2. 歴史的、統計的および科学的調査を行う団体は、以下の場合においてのみ、個人データの発表もしくは公開が許される。
2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:

(a) データの対象者が第 7 条に定める条件に基づいて同意した場合
(a) the data subject has given consent, subject to the conditions laid down in Article 7;

(b) 個人データの公開が、調査結果の提示に必要な場合、またはデータの対象者の利益、基本的権利または自由が侵害されない範囲において、調査の支援となる場合、もしくは
(b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or

(c) データの対象者が当該データを公開している場合
(c) the data subject has made the data public.

3. 欧州委員会は、第 1 項及び第 2 項の目的のために個人データの処理に関する基準と要件

を詳細に規定することに加え、データの対象者の情報に対する権利および情報へのアクセスに必要な制限を定め、かかる目的におけるデータの対象者の権利への保護措置と要件の細部を制定する目的で、第 86 条に従って委任法令を採択する権限を与えられるものとする
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.

第 84 条 守秘義務
Article 84 Obligations of secrecy

1. 本規則の範囲において加盟国は、個人データ保護に関する権利と守秘義務の調和が必要かつ適切な場合において、職業上の守秘義務、もしくは国内法または同国内で管轄権を有する組織による規則によってそれに類する守秘義務が適用される管理者または処理者について、第 53 条(2)に定める監督機関による監督権を設定するために、特定の規則を採択することができる。これらの規則は、守秘義務が適用される活動において管理者もしくは処理者が取得した個人データに対してのみ適用されるものとする。
1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

2. 各加盟国は第 1 項に従って採択した規則について、最長でも第 91 条(2)に定める期日までに、それらに影響を与える以後の改定については遅延なく、欧州委員会に通知すべきものとする。
2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

第 85 条 教会および宗教団体への既存のデータ保護規則
Article 85 Existing data protection rules of churches and religious associations

1. 本規則発効時点において、教会や宗教団体もしくは集団がデータの処理に際して個人デ

ータ保護に関する包括的規則を定めている場合、それらの規則が本規則と調和するならば、その規則は効力を有し続けることができる。
1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.

2. 第 1 項に沿って包括的な規則を適用する教会および宗教団体は、本規則の第 VI 章に沿って、独立監督機関を立ち上げなければならない。
2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.

第 X 章　委任法令及び施行法
CHAPTER X DELEGATED ACTS AND IMPLEMENTING ACTS

第 86 条 権限委譲
Article 86 Exercise of the delegation

1.委任法令採択の権限は、本条に定める状況に限って付与されるものである。
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. 第 6 条(5)、第 8 条(3)、第 9 条(3)、第 12 条(5)、第 14 条(7)、第 15 条(3)、第 17 条(9)、第 20 条(6)、第 22 条(4)、第 23 条(3)、第 26 条(5)、第 28 条(5)、第 30 条(3)、第 31 条(5)、第 32 条(5)、第 336 条)、第 34 条(8)、第 35 条(11)、第 37 条(2)、第 39 条(2)、第 43 条(3)、第 44 条(7)、第 79 条(6)、第 81 条(3)、第 82 条(3)および第 83 条(3)の権限移譲は、本規則の発効日から期限が設定されるまでの間欧州委員会に付与されるものとする。
2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. 第 6 条(5)、第 8 条(3)、第 9 条(3)、第 12 条(5)、第 14 条(7)、第 15 条(3)、第 17 条(9)、第 20 条(6)、第 22 条(4)、第 23 条(3)、第 26 条(5)、第 28 条(5)、第 30 条(3)、第 31 条(5)、第 32 条(5)、第 33 条(6)、第 34 条(8)、第 35 条(11)、第 37 条(2)、第 39 条(2)、第 43 条(3)、

第 44 条(7)、第 79 条(6)、第 81 条(3)、第 82 条(3) および第 83 条(3)の権限移譲は、欧州議会もしくは欧州理事会による撤回がいつでも可能である。撤回の裁定により、その中で定める権限移譲は廃止される。これは欧州連合官報における裁定の公表翌日、もしくはそこに定める以降の日に効力を発するものとする。それは既に発行している委任法令の有効性に影響を与えるものではない。

3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.*

4. 欧州委員会は委任法令の採択後すぐに、欧州議会と欧州理事会に対して同時に通達を行うものとする。

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. 第 6 条(5)、第 8 条(3)、第 9 条(3)、第 12 条(5)、第 14 条(7)、第 15 条(3)、第 17 条(9)、第 20 条(6)、第 22 条(4)、第 23 条(3)、第 26 条(5)、第 28 条(5)、第 30 条(3)、第 31 条(5)、第 32 条(5)、第 33 条(6)、第 34 条(8)、第 35 条(11)、第 37 条(2)、第 39 条(2)、第 43 条(3)、第 44 条(7)、第 79 条(6)、第 81 条(3)、第 82 条(3)および第 83 条(3)に従って採択された委任法令は、欧州議会もしくは欧州理事会への通達から 2 か月以内に異議の通達がなされなかった場合、もしくは両者が期限までに欧州委員会に対し異議がない旨を通知した場合に効力を発するものとする。欧州議会または理事会は自らの主導で、この期間を 2 ヶ月延長できるものとする。

5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

第 87 条 委員会の手順

Article 87 Committee procedure

1. 欧州委員会は委員会によって補佐されるものとする。その委員会は、欧州規則(EU) No 182/2011 における範疇のものとする。
1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. 本項を引用する場合、欧州規則 No 182/2011 第 5 条が適用されるものとする。
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. 本項を引用する場合、欧州規則 No 182/2011 第 8 条が同第 5 条と併せて適用されるものとする。
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

第 XI 章　最終規定
CHAPTER XI FINAL PROVISIONS

第 88 条 指令 95/46/EC の廃止
Article 88 Repeal of Directive 95/46/EC

1. 指令 95/46/EC は廃止される。
1. Directive 95/46/EC is repealed.

2. 廃止される指令への参照は、本規則への参照と解釈されるものとする。欧州指令 95/46/EC の第 29 条に定める個人データの処理に関する個人保護作業部会に対する参照は、本規則で設立される欧州データ保護委員会への参照とみなす。
2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

第 89 条 欧州指令 2002/58/EC との関係および同指令の改定
Article 89 Relationship to and amendment of Directive 2002/58/EC

1. 本規則は、連合内の公共通信ネットワークにおいて現在利用可能な電子通信サービスの規定に関わる、個人データの処理に関連のある自然人もしくは法人に対し、欧州指令 2002/58/EC に定める同様の方針によりこの者達に課される特定の義務に加え、新たな義務を課してはならない。
1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

2 指令 2002/58/EC の第 1 条(2)は削除されるものとする
2 Article 1(2) of Directive 2002/58/EC shall be deleted.

第 90 条 評価
Article 90 Evaluation

欧州委員会は、欧州議会および欧州理事会に対して定期的に、本規則の評価および見直しに関する報告書を提出すべきものとする。最初の報告書は本規則発効より 4 年を超えない範囲で提出されるべきとする。以降の報告書は、以後 4 年おきに提出されるものとする。欧州委員会は必要に応じ、情報技術の発展や情報社会の進展状況を特に考慮に入れた上で、本規則改定ならびに他の法律との協調を視野にいれた適切な提案を提出するべきとする。この報告書は一般に公開されるものとする。
The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society. The reports shall be made public.

第 91 条 発効および適用
Article 91 Entry into force and application

1. 本規則は欧州連合官報内での発行を受けて 20 日目より効力を発するものである。
1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. これは［第 1 項の日付より 2 年］に渡って適用されるものとする。本規則は全加盟国に対して全面的な拘束力を持ち、直接的に適用されるものである。
2. It shall apply from [two years from the date referred to in paragraph 1]. This Regulation shall be binding in its entirety and directly applicable in all Member States.

ブリュッセルにて,
Done at Brussels,

欧州議会御中	欧州理事会御中
欧州理事会議長	欧州理事会議長
For the European Parliament	The President
For the Council	The President

個人情報の安心安全な管理に向けた社会制度・基盤の研究会 報告書

平成 24 年 3 月 30 日　第 1 刷発行

発　行：一般財団法人日本情報経済社会推進協会

〒105-0011　東京都港区六本木一丁目 9 番 9 号　六本木ファーストビル内

TEL 03-5860-7562　FAX 03-5573-0561　　http://www.jipdec.or.jp/