

2004年10月29日

金融分野における個人情報保護に関する  
ガイドライン(案)についての金融庁によるパブリック・コメントの求めに応じる  
在日米国商工会議所(ACCJ)  
プライバシー・タスクフォース及び金融サービス委員会の  
意見答申

ACCJは、個人情報保護に関する法律(以下「基本法」という)についての金融分野を対象としたガイドライン草案(「本ガイドライン」という)について論評する機会を与えられたことに感謝致します。我々は、この機会に、金融庁が本ガイドライン草案作成過程の透明性を高められていることを賞賛致したいと存じます。ACCJは、個人のプライバシーとして正当に期待される内容を保護するために基本法が必要かつ健全な処置であると信じておりますが、またその一方で個人データを取り扱う会社がビジネスの現実にあわせてその運用を組み立てる柔軟性をもつ必要があることを考慮しております。各省庁により公布される予定のガイドラインは、基本法の一般的な規定を解釈する際に不可欠となるはずであり、個人情報保護の保護に加えて情報の適切かつ効率的な利用の価値に及ぶ基本法の適切なバランスに従うべきものです。このような考えをもって、ACCJは、本ガイドラインについて以下の意見を申し述べたいと存じます。

省庁間の調整

基本法の枠組の下では諸省庁が特定分野のためのガイドラインを定める責任があります。故に、これらガイドラインの作成に際しては省庁間の強力な調整が規則とガイドラインの相反を避けるために不可欠です。特に、すべての省庁が作成するガイドラインが互いに整合性のあるものであることが重要となるでしょう。例えば、現在起草されているものでは、金融庁ガイドラインと厚労省ガイドラインがともに、金融庁が管轄権を有する団体の従業者に適用されます。すべての省庁がそのそれぞれのガイドラインで用いている定義及び用語、並びに課している義務が、すべてのガイドラインを通じて一貫しているべきです。また、執行の過程で省庁間の強力な調整があることも重要でしょう。管轄が共通している場合は、省庁は、見解を統一し、共通の決定又は裁定を下すべきです。事業者は、省庁間の差異を解決する責任を負わされるべきではありません。可能な範囲で、かかる決定又は裁定は公表され、公開されて、事業者が諸省庁の解釈を理解し、その事業を組織的に進める際にかかる解釈に信頼できるようにすべきです。金融庁は、調整された「ノーアクション・レター」手続きを積極的に用いるように他の省庁と協働して、これにより事業者が諸省庁と相談し、かかる事業者に対する行政措置

をとらないとの省庁の決定を信頼することができるようにするべきです。かかる手続きは、基本法及びその関連のガイドラインを執行するための透明で予見可能なシステムを促進するために不可欠のものです。

## 本ガイドライン草案の実体的規定

### 個人情報定義(第2条)

以下に述べる理由により、我々は、金融庁に対して、(a)事業及び職業の情報、(b)公に入手できる情報及び(c)匿名化又は暗号化されたデータを本ガイドラインの第2条に定義されている「個人情報」から除外することを求めます。

#### (a) 事業及び職業の情報

我々は、金融庁が、個人情報定義から、名刺に記載されている情報等の「事業の運営を含み、企業、専門的能力若しくは公的立場にある個人を特定する情報、又は個人の職業的若しくは公的な責任及び活動及び関連の取引を説明し、意図的なビジネスの目的のために使用される情報」を除外するようにお勧めします。その代わりに、金融庁は、電話帳及びナビゲーション・システム(経産省の経済産業分野を対象とするガイドラインのII 1(4); 基本法の第2条第4項)の取扱いに適用される除外規定をかかるとして拡張して適用することができるでしょう。その場合は、個人データであるとはみなされず、故に、事業者に対して課される義務は適用されません。

ビジネスマンの中でビジネスの連絡情報が意図的なビジネス上の目的のために交換されている場合、個人は情報がそのように使用されると期待しているのですから、一般的に言って、同意を得ることは非現実的であり不必要です。その上、意図的なビジネス目的のための連絡先又は職業に関する情報の収集、使用及び移転について通知及び同意の義務を課すことは、極めて時間がかかり、費用がかさむものの、これに見合うプライバシー保護を得られないような負担となる恐れがあります。この要件が日本的な販売方法及びビジネス上の紹介の性質と相反すると言っても過言ではないでしょう。例えば、外国の金融サービス会社は一般的にグローバルな顧客関係管理(CRM)のデータベースを使用しており、これには、顧客関係、潜在的顧客等の情報を日本の内外の関連会社と共有する必要がありますが、かかる会社は、年金基金又は機関投資家等の他の団体を代表する者からビジネスの情報を頻繁に受け取っています。かかる情報は、本ガイドラインの適用範囲から除外されるべきです。

本ガイドラインが事業及び職業上の情報に関する除外を限定された事由でのみ認められるなら、除外規定の範囲は著しく狭くなり、例えば、かかる個人に対して情報やマーケティング資料を送ることも許されなくなるでしょう。もし名刺に含まれる情報をすべて除外できない場合、個人情報定義から特定の情報(例えば、所有者の名前(但し役職を除く))を除外できるようにするべきです。

## (b) 公に入手できる情報

公に入手できる情報は個人情報の定義から除外されるべきです。公に入手できる情報とは、公衆が入手できるように個人が故意に公開若しくは許可した当該個人についての個人情報、又は、公開されている政府の記録から適法に入手しアクセスした個人情報、ジャーナリズムの報道、又は法律により公衆が入手できるように要請されている情報を意味します。いったん情報が公開されれば、かかる情報を正しく使用することに制限があるべきではありません。

## (c) 匿名化又は暗号化されたデータ

匿名化又は暗号化されたデータは、個人データの定義から除外されるべきです。個人特定が可能な情報をすべて除去するか又はアクセス不可能とした情報は、研究及びその他の統計上の目的のために不可欠です。従って、匿名化又は暗号化された（かつ受け手が暗号解読のキーを有していない）情報は、個人を特定するために利用できる情報をもはや含んでいないので、個人情報の定義から除外されるべきです。

### 通知(第 3条及び第13条)

本ガイドラインにおける利用目的特定の要件(第3条)及び第三者に対する情報提供の制限(第13条)は、事業者に対して、不必要かつ過度の負担となる通知義務を課すものです。草案では、(目的及び/又は第三者のカテゴリー又は種類を説明することではなく)それぞれの目的、並びにすべての第三者、共同パートナー、及び信用情報機関の会員が個別に特定されなければなりません<sup>1</sup>。これは、次の理由で問題となります。

1. 金融機関が別の団体と協働したり、別の第三者とデータを共有したりするように選択した場合は、目的が事前に定められており団体が従前の団体と類似(又は同一のカテゴリーに属する)としても、新たな通知(及び同意)が必要とされるでしょう。
2. この要件は、事業者に対して、OECDガイドライン及びEU指令で用いられているよりも高い基準を課すものであり、ビジネスの現実に適合しません。
3. この要件は、過去数年間において金融サービス業界が企業の負担によって築き上げてきた基準や慣行に反するものです。これらの基準や慣行は個人情報を保護するという目的を十分に果たしています。
4. 草案では、かかる要件の結果として通知が過度に詳細で長大なものとなり、個人が容易にアクセスしたり読みこなしたりできそうもないものとなり、結果

---

<sup>1</sup>信用情報機関からの信用情報にアクセスする会員会社の名称を、会員資格の基準とともに、ある箇所に記載して、かつその更新を続けなければなりません。より実現可能性のあるアプローチとしては、信用情報機関に対して、会員会社及び会員資格の基準の最新リストを掲載する中心ホームページを立ち上げるように奨励し、個人情報を取り扱う事業者がこれに言及するようにすることが挙げられるでしょう。

的に、事業者及びその従業者に対する不必要かつ不合理な負担となる膨大な通知を生み出すこととなるでしょう。

ある団体が第三者に情報を提供したり、又は情報の共同使用に参加したりする際には、その団体は、消費者に対して新たな通知を与える義務なくしてサービス提供者を変更する柔軟性を有していなければなりません。例としては、第三者である サービス提供者が何らかの理由で事業を中止し、故に、代わりのサービス提供者と同一のサービスを提供させる契約を結ぶ場合に、通知の要件が課されるべきではありません。金融機関は、バックオフィス・サービスの提供を目的として第三者に情報を提供していると開示するよう要請されるべきですが、かかるバックオフィス・サービスの提供のために利用すると選択した第三者の具体的な名称を開示するよう要請されるべきではありません。

我々は、金融庁に対して、第3条第1項に例が引かれているような、使用の種類又はカテゴリーを説明すれば十分であり、事業者が個別の使用について(使用のカテゴリー以上に)詳細で項目別のリストを提供する必要はないということを明確にするように求めます。かかる要件のために、申込書や取引条件を詳細にカスタマイズする必要が生じ、極度の負担となるでしょう。また、我々は、金融庁が、かかる利用目的の説明をクレジット又は別の金融商品若しくはサービスの申込みの際に顧客が署名する申込書により提供でき、別の通知は不要であるということを明確にするようにお勧めします。

一般的に通知の時期については、可能な場合は常に、事前に通知するべきであることに賛成致します。ただし、事前に、又は収集の際に通知を与えることが技術的に不可能であるか実際的でない場合があります。故に、本ガイドラインでは、適当な状況で、事後の通知が受け入れられると明確に認めるべきです。例えばクッキーの場合は、クッキーが稼動される後にならなければ通知を与えることは技術上不可能です。そうしなければ誰に通知するかが分からないからです。同様に、消費者がATMを利用する場合は、取引を開始したり通知の言語を決定したりするためにカードを挿入しなければならず、金融機関による情報の収集はその後に行われます。従って、金融機関は、情報の使用方法についての通知を、情報がいくらか収集された後にならなければ通知することができません。

また、利用目的を、契約書、申請書又はその他の書類における個人情報を取得する前に開示する必要がないこと(つまりかかる情報を取得する時に開示すればよいこと)を明確にするために、第8条第2項を修正することをご提案させていただきます。

### **同意(第3条、第4条、第5条及び第13条)**

基本法は、ほとんどの状況で、オプトアウト同意が適当であると規定しています<sup>2</sup>。これとは対照的に、本ガイドラインは、基本法がオプトアウト同意を受け入れるべきものとみなして

<sup>2</sup> 例えば、基本法の第18条第3項では、先に収集された情報の利用目的が変わった場合、団体は、個人に対して通知するか、新たな利用について公表をすれば足りると規定しています。これはオプトアウト同意に相当し、個人

いる多くの場合に、オプトイン同意を要求しているという点で、基本法と不一致があるように思われます。とりわけ、

- 第4条は、同意が必要とされる場合は常に、書面のオプトイン同意でなければならないと示しているように思われます(タッチスクリーン・パネルの場合の「確認のタッチ」を含む)。これは、金融機関にとって極めて負担の重い義務となり、消費者の負担を増すこととなりますが、これにより有意義なプライバシー保護が高められることはないでしょう。第4条は、オプトアウト同意の例を含めるように修正されるべきです。例えば、情報が別の目的に使用されたり又は第三者と共有されたりする可能性があるが、本人が会社に通知することによりかかる共有又は利用の変更を忌避できるという大胆な開示によるオプトアウト同意の例です。疑念を避けるために述べますが、当初の契約にすでに定められている目的のために情報を利用するにあたっては、オプトアウト同意ですら必要とされないこともまた、明確にするべきです。
- 第5条第1項(利用目的による制限)は、目的に変更がある場合は常にオプトイン同意が必要とされると示唆しています。第3条第3項並びに第13条第1項及び第3項は、情報が特定の利用目的のために使用されるときはオプトイン同意が不要である(例えば、通知又は公表の中で指定された目的)と明確になるように修正するべきです。
- 第3条第3項は、与信目的のデータの収集、使用とマーケティング目的のそれでは、別個のオプトイン同意が必要とされると示唆しているようです。本ガイドラインではまた、その「取引上の優勢な地位」を用いることにより、個人に対して受け入れ不可能な条件を課す種類の契約上の文言があると示唆しています。かかる懸念を生ずる種類の契約上の文言は明確ではありません。個人がその個人情報を与信目的で収集及び使用されることに合意しなければならないと申込書に記載できるよう、事業者は許可されるべきです。さもなければ、顧客に対して、望まれる資金を提供することは不可能でしょう。
- 第13条に基づき、信用情報機関を含む第三者とデータの共有をするためには、オプトイン同意が必要とされます。これは、金融機関にとって特に問題となるという印象を受けます。何故なら、不良債務のある個人に対して、かかる情報を信用情報機関と共有することを禁ずることを可能にし得ると思われるものだからです。その上、経産省の信用分野におけるガイドラインでは、対照的に、経産省の管轄下にあるかかる団体に対して不当な利益を生ずるかかかる共有を許可しているのです。さらに、勘定分析を目的として信用情報機関及びその会員会社と情報を共有することは、同意(オプトアウトであるかオプトインであるかを問わず)を必要とせず、顧客に対して明確に開示すれば足りるとするべきです。とりわけ、過度の貸付に反対する国家政策(例えば、貸金業法第13条)に照らせば、信用情報機関は、顧客の財務情報の共同利用者として認められるべきです。

---

によるいかなる積極的行動も必要とされません。同様に、第23条では、一般的な事項として、個人情報は、本人の同意なく第三者に提供されるべきではないと規定しています。しかしながら、第23条第2条では、個人に通知が与えられた場合は、当該個人が提供しないように求める権利を有している限り、個人情報を第三者に開示できる(すなわち、オプトアウト)と定めています。

特に、情報を収集する団体と情報を利用する団体が同じである場合、オプトイン同意を要求することに、個人情報保護にとって特段のメリットがあるようには思えません。基本法に定められている適正バランスを維持するためにも、オプトアウト同意を許可するように上述した条項を修正することをご提案させていただきます。

### 第三者に対する情報の提供(第13条)

基本法とは対照的に、本ガイドラインは、その第三者の定義から、支配株主、又は代理人としての行為を行う者、共同のマーケティング活動に従事する者、又は合併の際に現存の事業者に代わる者を除外していません。我々は、金融庁に対して、本ガイドラインでは第三者の定義にはこれらの例外があり、かかる団体に対して情報を提供する際にオプトイン同意が必要とされないと本ガイドラインにおいて明確にされるように求めます。

本ガイドラインにおいてはまた、その第三者の定義又はその第三者同意要件の免除のいずれかにより、オプトアウト同意の使用によりクロス・マーケティング目的のためにデータを関連会社と共有できると明確に示すべきです。クロス・マーケティングを目的としてデータを関連会社と共有することは、関連のない法人の間で共同のマーケティング上のイニシアティブをとることに似ています。さらに、事業者が、同意よりはむしろ一般的な開示(事業者のウェブサイト等)により、情報が共有される関連会社の名称を増やしたり修正したりできるようにすべきです。

本ガイドラインでは、顧客が求める取引を実現するために必要な場合における信用情報機関(上記)、その他の銀行若しくは団体との共有、支払いの取立て若しくは延滞勘定の解決を担当する第三者との共有<sup>3</sup>、合併の場合(下記)、又は再保険会社に関する場合等、一定の種類<sup>3</sup>の第三者とのデータ共有に対して、同意要件を免除すべきです。詐欺の調査やその他の身元調査の目的で利用されるデータベース提供者もまた第三者とみなされるべきではありません。なぜなら、これらの調査は、通常、支払能力以外の目的でも行われるからです。例えば、顧客情報は収集されてデータベース企業と共有され、詐欺を削減したり、顧客の通常の支払傾向、口座の悪用及び過度の引き出しを理解したり、口座に問題がある場合に顧客に連絡したりするために利用されます。

保険業においては、適切な業務を目的として、個人情報を再保険会社と共有するためにオプトイン同意が必要とされるべきではありません。情報を共有する目的は、初めの保険会社が先に引き受けた義務を果たすことであり、故に、本人のさらなる同意を得ることが必要とされるべきではありません。この状況においては、再保険当事者は、第三者というよりもむしろ外部委託先のパートナーとしての役割を果たしています。もし金融庁が再保険当事者を「第三者」とみなすのであれば、組織が個人に対して通知を行った場合又は使用目的を公表した場合に、個人情報<sup>3</sup>がオプトアウト同意によりかかる目的のために開示できることを明確にするべきです。

---

<sup>3</sup>債務の解決のために第三者と協力する責務は、すでに金融庁自身のガイドラインにより認められておりますので(例えば、MLBL第21条 ガイドライン、セクション 3-2-7)、ガイドラインは、その他の適用される法律に基づくかかる既存のガイドラインとの調和をはかるべきです。

第13条第4項及び第13条第6項に関しては、「本人が容易に知り得る状態」に置くために、第三者又は共同利用者の商号又はホームページ・アドレスを開示すれば十分であるかどうかを、金融庁が明確にされるようにお勧めします。第三者と共同利用者を別個に記載する必要があるでしょうか。

第13条第3項は、「金融分野における個人情報取扱事業者は、個人信用情報機関から得た資金需要者の返済能力に関する情報については、当該者の返済能力の調査以外の目的に使用することのないよう、慎重に取扱うこととする」と定めています。個人信用情報機関による情報利用を一律に禁止することは、基本法の、通知及び個々の同意に基づいて情報が適正に使用されるべきであるという方針と相容れないと考えられます。従って、我々は、金融庁に対して、個人信用情報機関が資金需要者の返済能力の調査を超える利用目的を当該資金需要者に通知し、又は公表した場合、一それにより、資金需要者は適切な通知を受けることができるのですが一上記利用制限が適用されないこと、また、オプトアウト同意を使用することにより、当該情報にかかる他の利用目的のために開示できることを明確にするよう求めます。我々はさらに、金融庁に対して、個人信用情報機関が資金需要者の返済能力の調査を超える利用目的を当該資金需要者に通知し、又は公表することを前提として、事業者が個人信用情報機関から受領した資金需要者の返済能力の調査に関する情報以外の情報を利用できること、また、オプトアウト同意を使用することにより、当該情報にかかる他の利用目的のために開示できることを明確にするよう求めます。

最後に、ACCIは、金融庁に対して、第13条第5項の意味を明確にされるよう求めます。何故なら、同項の導入部の論理によれば、現在の同項の結論とは別の結論が導かれると思われるからです。

### 統合及び合併(第5条)

金融サービス会社の間での合併においては、買収側が、ターゲットとなる会社の顧客情報を評価過程の一環として調査するのが標準的な慣行です。潜在的投資家又は会社資産の購入者は、意図される取引に関連する精査目的で、かかる情報を調査する必要があります。同じことは、物品及びサービスの購入のために資金提供による解決を提供する金融パートナーに当てはまります。第5条第2項に基づくとみられるものですが、非開示契約に服する顧客の個人情報の共有及び使用が禁じられた場合は、金融サービス会社の間での買収合併活動の重大な妨げになるでしょう。さらに、会社が顧客に通知してその同意を得る必要があるとすれば、かかる開示は「インサイダー取引」のリスクを高めます。

故に、我々は、金融庁に対して、本ガイドラインにおいて、事業者が個人情報を次の者と共有するために通知及び同意を要しないと明確にされるように求めます。すなわち、(i) 意図される取引に関連する精査目的で、かかる情報を調査する必要がある潜在的投資家又は会社資産の購入者、又は、(ii) 事業者により売却される物品の購入のために、資金提供による解決を提供する団体、と共有する場合です。

### 本人に対するアクセス/開示(第15条)

本ガイドライン第15条では、利用目的がいったん達成されたら、事業者は、該当する個人情報情報を破棄するべきであると定めています。事業者が、利用目的が達成された後に受ける顧客からの問い合わせ又は事業者と顧客間の契約上の法的問題に対応できるよう、利用目的以降も(例えば、保険契約の期間満了以降も)情報を保持できることを金融庁が明確にされるようお勧めします。

情報へのアクセスに関しては、利用目的(例えば保険契約の期間満了)がいったん達成されたら、単にその情報へのアクセスを提供する目的のために、事業者はかかる情報を維持する必要はないと金融庁が明確にされるようお勧めします。我々はまた、個人による個人情報へのアクセスは、情報が利用目的を達成するために使用されている期間に限られると金融庁が明確にされるように、金融庁に対してお勧め致します<sup>4</sup>。その上、業務の実施に「著しい支障を及ぼす」場合においてアクセスを与える必要がない事由について、本ガイドラインではより詳細な説明をするべきです。文言の意味が不明瞭です。例が一つだけ与えられていますが、これは、求められた情報量が開示の理由に対応していない事例に関するものです。別の例として、取引の完了の1-3年後に取引データにアクセスしたいという要望が出された場合があり得るでしょう。この場合、このような保存されたデータすべてに対するアクセスを許可するのにかかる費用は法外なものとなり、金融機関に対する不当な負担となるでしょう。

また、個人情報取扱事業者が本人から求められた場合、保有する個人データを「遅滞なく」開示しなければならないという文言に関して、金融庁が「遅滞なく」という語の意味を明確にして下されば助かります。曖昧で、個々の検査官の主観的な解釈に従う本ガイドラインを金融庁が作成されないことは極めて重要です。本ガイドラインでかかる曖昧な規定を設けることにより、金融庁は、規定の検査の際に、検査官と金融機関の間で深刻な衝突を生ずるリスクがあるでしょう。

### 機微情報の収集(第6条)

本ガイドラインは、機微情報(「政治的見解、信教(宗教、思想、信条)、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴」として定義されます)の収集を禁止しています。本ガイドラインが金融機関の人員(すなわち、従業者及びその他の労働者)に適用されるとすれば、かかる禁止は、従業者についての厚労省のガイドラインと直接に抵触することがあり得ます。機微情報の収集を禁止することは、厚労省のガイドラインに抵触する上に、重大な問題を生ずるでしょう(金融機関が、身元調査を行い、おそらくは生命保険又は健康保険を提供又は管理し、障害者を収容し、申込者のフロー・データを収集

---

<sup>4</sup> 金融機関は、記録を目的として、取引のデータを長期に保管します。しかしながら、かかる保存された取引データすべてに対するアクセスを許すためにかかる費用は莫大なものとなるでしょう。従って、取引データに対するアクセスの請求は、取引が完了した後の合理的な期間(例えば、1-3年)に限定されるべきであり、情報の請求はすべて、かかる請求が金融機関に対して不適當な負担とならない場合にのみ受け入れられるべきです。その上、情報を収集された目的のために使用される期間を超えて長く保持しないという、アクセス請求と対立するような、基本法に基づく義務があります。従って、基本法は、金融機関が、もはや必要でなくなった情報を削除するように奨めておりますが、その意味するところは、アクセスは、いったんこの情報が削除又は匿名化されれば不可能となるということです。

し、労働組合の組合費の集金及び支払いをなし、国内のパートナーシップ給付を提供することができなくなり、医療機関や医療組合を介したローンの提供を制限し、特定の慈善団体への言及及び寄付を生じさせる等)。また、機微情報の収集は、障害をもっている顧客に対してより良いサービスを提供するために必要かもしれません。

これらの制約は、とりわけ金融事業者が貸付け業務を担当する従業員がその責務にふさわしいことを確保する要件(例えば、貸金業法第24条の7、第13条の3)に照らして、問題となり得るものです。故に、本ガイドラインは次のいずれかを行うべきです。すなわち、(1)雇用の状況においては、かかる情報の収集及び選択的な使用を明示に許可すること、(2)かかる使用が「法令に基づく」収集の例外にあたることを明確にすること、(3)金融機関の従業員及び労働者の個人情報には適用されないものとする、(4)オプトアウト同意に基づく顧客のための機微情報の収集を許可すること。

「法令に基づく」収集の例外には、外国の法律又は規則が含まれるべきです。例えば、米国の生命保険会社は、米国の税務法令を遵守するために、その保険証券保有者の国籍についての情報を収集するようしばしば要請されます。

さらに、ATMや銀行内において、安全保護のためのビデオカメラで情報を収集することは、個人の人種や民族などの機微情報がかかるビデオカメラによって収集されるとしても、明確に許可されるべきです。

最後に、第6条第1項第7号は、保険会社を含む金融会社に対して、顧客の同意を得てその機微情報を使用又は第三者と共有することを、事業の遂行に必要な範囲で許可していますが、その一方で、我々は、とりわけ団体が、新たな利用及び個人情報が第三者に開示され得るという事実について、個人に対して通知を与えたり又は公表を行ったりする場合は、かかる同意がオプトアウト同意であるべきだと明確にするよう、金融庁に対して求めます。例えば、住所などの情報は、不正防止のために金融サービス企業によって日常的に収集されるものであり、免許証をコピーするなどして行われています。よって、金融庁は、かかる情報が第6条第1項第7号に基づき、オプトアウト同意により収集できることを明確にするべきです。

### **データ内容の正確性の確保(第9条)**

本ガイドラインは、いったん利用目的が達成されたら情報を破棄しなければならないと定めています。この要件は、データの完全な破棄又は削除が事実上不可能であるため、技術的に実現できないものです。例えば、データは、しばしばオフサイトで貯蔵されるバックアップ・メディアに貯蔵されるのがほとんど常態となっています。データのシャドウ・コピーもコンピュータ・システム内部に存在するでしょう。これに代わって、本ガイドラインが確認すべきことは、事業者がデータを抑制し、又は積極的な活用から除外し、又は可能な箇所すべてからデータを削除できるということです。

本ガイドラインはまた、個人データを破棄又は削除すれば事業者が適用される法律に違反することになる場合(例えば、法律により、事業者が、定められた期間、その事業の運営にとって重大な一定の情報のコピーを保持しなければならないと規定されている場合)は、破棄又は削除が行われるべきではないと明らかにするべきです。

第9条に基づく、個人情報取扱事業者は正確な個人情報を維持しなければならないとの意図された責務に関しては、事業者が法律に従って個人情報を本人から受け取ったが、かかる情報が申込書により本人から受け取った情報に反する場合における事業者の適切な対応について、本ガイドラインで明確にするべきです。万一、団体が本人により提供された情報を変更して法律に従って提供されたものに合わせたとすれば、あるいは本人により提供されたものとして当該情報を保管したとすれば、どうでしょうか。

第9条はまた、個人情報取扱事業者が利用目的に応じて保存期間を定めなければならないと述べていますが、本ガイドラインはまた、第3条第1項で利用目的が具体的でなければならないと強調しています。事業者に多くの異なる利用目的があることがあり得るため、我々が想像するのは、異なる利用目的に対して異なる保存期間を定めなければならないと、従って、第9条を遵守するために、同一の情報を同一の本人のために異なる期間の間繰り返し保管するように要請されるという状況です。本ガイドラインでは、これが不要であると明確にするべきであり、また、事業者は利用目的ではなく、情報の種類によってその保有を決定できることを明確にするべきです。

### 安全管理措置(第10条)

本ガイドラインが定める安全管理措置は、基本的事項についての規定であり、かつ具体的で詳細な安全義務を含まないものであるべきです。添付No. 5は、「最善の慣行」基準として提示されるべきであり、本ガイドラインは、これらの示唆に従う法令上の義務を負わないと明確に定めるべきです。

第10条第6項において、本ガイドラインは、事業者が、「個人データの取扱い状況を確認できる手段の整備」等の具体的な「組織的安全管理措置」をとらなければならないと定めています。「確認できる手段」の意味は不明確です。例えば、これは、情報システムのことでしょうか、それとも電子的なソフトウェア又はハードウェアのシステムのことでしょうか。あるいは、チェック・シートか、又は、法令遵守担当者を配置する等の生身の人が関与する確認手段のことでしょうか。また、第10条第6項第1号により、本ガイドラインは、個人情報を使用する金融サービス会社の各部署に個人データ管理の担当者を任命することを意図しているのでしょうか、それともこれは、一人の個人が会社全体にわたって使用される個人データの管理を担当するという意味でしょうか。

### 雇用契約(第11条)

第11条第3項第1号が、会社内で仕事が変わり、故に新しい資格では個人情報を使用及び共有する理由がなくなった現存の従業者にのみ適用されるのか、それとも契約の範囲が現在従業者及び退職した従業者に及ぶものでなければならないと示唆しているのかを、金融庁が明確にされるようにお勧めします(混乱は、「職を退いた者」という語の意味に関するものです)。

本ガイドラインでは、従業者との個別の雇用契約について、金融機関による雇用の間に利用目的以外のいかなる理由でも個人情報等を第三者と共有しないようにすることを要請しています。契約の締結をこのように強制することは非現実的です。既存の従業者について、従業者が契約に署名することを拒否した場合はどうなるのでしょうか。署名の拒否を理由として雇用を終了させることが出来るのでしょうか。かかる拒否は、正当な目的による終了とみなされるのでしょうか。我々は、事業者がこのような義務を自身の就業規則に記載することによって当該条項を満たすことを本ガイドラインが許可することをお勧めいたします。

金融機関を退職又は辞職した者である従前の従業者に関しては、いったん雇用を離れてしまった者の行動について、事業者は、ほとんど支配力を有していません。雇用後の行動を規制する契約上の規定は、同様に非現実的です。本ガイドラインは、これがすでに退職又は辞職した従業者には適用されないと明確にするべきです。

その上、本ガイドラインにより適用される安全管理措置と同様に、本ガイドラインにより適用される従業者の監督措置は、高レベルであり、かつ具体的で詳細な安全義務を含まないものであるべきです。本ガイドラインの添付No. 5は、「最善の慣行」基準として提示されるべきです。さらに、金融庁が従業者の監督に関連してさらに採用するガイドラインは、「最高の実行」となるべきです。従業者についての規定はまた、厚労省ガイドラインと一致しているべきです。

### 開示等の求めに応じる手続き(第19条)

すべての支店又は販売事務所で開示の請求に応ずる手段を定める代わりに、本ガイドラインは、顧客がかかる請求をなし得る場所を、一箇所又は非常に限られた数だけ設置することを許可するべきです。

### 漏洩事案への対応(第22条)

第22条では、漏洩事案に対して適用される措置は、データが滅失又は毀損されたのと異なり、漏洩した場合にのみ適用されると明確にするべきです。不注意によりデータが漏えいした場合の対応と、不注意によりデータが毀損した場合の対応はかなり異なります。

下記の修正をご提案させていただきます。

第22条第1項 金融分野における個人情報取扱事業者は、個人データの重大な漏えいが発生した場合は、監督当局に直ちに報告することとする。

第22条第2項 金融分野における個人情報取扱事業者は、個人データの重大な漏えいが発生した場合は、二次被害の防止及び同様の事態の回避に必要な範囲で、事実関係及び再発防止策等を公表するために最大限努力することとする。

第22条第3項 金融分野における個人情報取扱事業者は、個人データの重大な漏えいが発生した場合は、速やかに漏洩等の事実関係等について漏洩等の対象となった本人に通知するか又は公表することとする。

## 本ガイドラインで取り上げていない論点

### 日本国外で収集された情報

金融庁は、本ガイドラインが、日本で収集されたものではなく、加工及び使用のために日本に移転された個人情報に適用されるのか、それとも日本で収集及び使用される情報のみ適用されることになるのかを明確にするべきです。例えば、個人情報が加工及び使用のためにヨーロッパから移転された場合は、ヨーロッパのプライバシー規則と日本のプライバシー規則(例えば、通知及び同意)のどちらが適用されるのでしょうか、又は両方の制度が適用されるのでしょうか。基本法による義務の範囲をかかえるデータに拡大することは、過度の負担となり、日本への投資意欲をそぐこととなるでしょう。金融庁はまた、本ガイドラインが、事業者の所在地が日本国外にあり、データの加工が日本で単にサービスの提供として行われている場合(例えば、データベース貯蔵、ITサポート・サービス、及びコールセンター・サービス)に適用されるのかを明確にするべきです。

### 義務規定又は任意規定

本ガイドラインでは、多くの義務規定を定めていますが、任意の規定も数多く見られます。これら任意規定は、しばしば大企業による最善の慣行を表現しています。我々の信ずるところでは、本ガイドラインは、政府がすべての事業者に対して強制したいと考える規定に限定されるべきです。事業者は、義務規定を超える処置が必要な場合、自ら、その運営に適切な処置を自由に決定するべきです。

それ故に、金融庁は、その管轄に属するすべての会社に対する義務とされるべき規定のみを本ガイドラインに記載するようにお勧めします。ただし、金融庁が任意のガイドラインが必要であると考えられる場合は、金融庁は、任意規定が示すのは事業者が基本法を遵守する方法の例、又は最善の実行例であって、基本法を遵守するための唯一の方法を示すのではないと明示するべきです。

本ガイドラインはまた、特定の提案を採用しないことが、すなわち十分な安全性を提供していないこと、またはその業界における最善の慣行を行っていないことを意味するわけではないと明確にするべきです。その上、推奨規定があるということは、検査官に対して、監査/検査に際して過度の裁量権を与え、検査の手続きを土台から損なう恐れがあります。検査官が検査し評価しなければならない点を明確にするべきであり(例えば、義務規定)、裁量とすべきではありません。本ガイドラインで「任意」とされているとしても、行政及び民間の民事執行においては、これらの任意基準が、行政当局及び法律を解釈する裁判所の見方により、任意条項に従わなかった被告に不利な証拠となることもあり得ます。

## 外国の法律又は条例の遵守

本ガイドラインでは、外国の法律又は条例が、基本法に定める「法令に基づいた」例外(第16条第3項第1号)、第18条第4項第3号、第23条第1項第1号及び第25条第1項第3号等)となることを明確にするべきです。本ガイドラインでは、国際的な団体が日本以外の国の法律又は規則に従って情報を開示するように要請された場合、かかる開示は、当該用語が基本法に用いられる通りに「法令に基づいた」開示であるとみなされると明確にするべきです。換言すれば、日本以外の国の法律又は条例の遵守は、法令に基づいた開示であるとみなされるべきです。

## 遡及的な適用

本ガイドラインは、金融サービス会社がすでに収集した個人情報に適用されるか否かについて明確ではありません。もしそうなら、極度の負担となり、金融サービス会社は何百万ページにのぼる書類やCRMデータベースから個人情報を削除しなければなりません。本ガイドラインが遡及的な効果を有しないと金融庁が明確にされるようにお奨めします。

## さらに明確化が必要な条文

### 本ガイドラインの適用範囲

金融庁は、保険会社の販売代理店等の団体により取得された情報がかかる保険会社等と共有されていない場合は、本ガイドラインの適用範囲に該当しないと確認するべきです。

## 取得に際しての利用目的の通知等(第8条)

我々は、金融庁に対して、第8条第3項において、「取得の状況から見て利用目的が明らかであると見とめられる場合」として、事業者が無人契約機を介して個人の画像データを取得する場合を追加例として記載することを求めます。