

宛先： 東京都千代田区永田町1丁目6番1号  
内閣府国民生活審議会個人情報保護部会

送信者： 在日米国商工会議所(ACCJ) プライバシータスクフォース  
[住所] 東京都港区麻布台2-4-5メソニック39MTビル10階  
[Tel] 03-3433-5381 [Fax] 03-3433-8454  
[連絡先] 在日米国商工会議所渉外室日本政府担当マネジャー安田美穂

日付： 2006年10月27日

題名： 「個人情報保護に関する主な検討課題」への意見・提案

ファクシミリ通信 03-3581-0517

「個人情報保護に関する主な検討課題」と題する文書に対し意見提出の機会をいただき感謝申し上げます。以下のとおりコメントさせていただきます。

#### 1. 1 (1) 事業者の個人情報保護の取組における格差があることについて

要旨：コンプライアンスを広く促進するには、プライバシー規制は、プライバシーへの合理的な保護を目指した最低限必要なものにとどめるべきである。ガイドライン等は必須条項のみを定めるべきである。また、ビジネス上の連絡先情報および公知の情報には、個人情報・個人データに適用される通知・同意取得義務が適用されるべきではない。

コメント：プライバシー規制へのコンプライアンスを広く促進するには、明確で一貫性があり、分かりやすい、予測可能なガイドラインが不可欠である。ガイドラインは、複雑で規範的になるほど、その規制へのコンプライアンスの普及が困難となる。例えば、多くの事業者が、複数の省庁ガイドライン（「ガイドライン等」）による制約を受けている。さらに、これらガイドライン等の多くは、必須義務および任意規定のいずれをも含んでいる。これは特に安全管理規定に当てはまり、この結果、コンプライアンスの重要性を真摯に受け止め、今後の実施の方向性を見込んでガイドライン条項を厳格に解釈する事業者と、同じ条項を単に任意のものとして受け止める事業者とで不公平な土壌が生み出されることとなる。これらの条項の膨大な量と過度に詳細で規範的な性質が、ガイドラインへのコンプライアンスを一層困難にしている。プライバシー規制は、可能な限りプライバシーへの合理的な保護を目指した最低限必要なものにとどめるべきである。特にガイドライン等は、すべての事業者に必須義務とされる条項のみを定めるべきである。このような取組みにより、より広く、円滑なコンプライアンスが促進される。

個人情報保護法の適用範囲に関するガイドライン等の解釈もまた、コンプライアンスの普及の妨げになっていると思われる。例えば、ガイドライン等では、個人情報にはビジネスおよび職務情報ならびに公知の情報を含むとする拡大解釈を採用している。例えば、消費者データまたはビジネスデータ双方に見合ったレベルのプライバシー保護を設定せず、収集、利用および転送についての通知および同意等同じ保護要件を適用するとすれば、時間、費用を要し極めて負担が大きい。個人のビジネス上の連絡先情報は、公開され自由な利用に供されることが多い。

ビジネスデータに対しても同様の保護を適用することで、当該情報の共有を制約し、事業者が日常業務を行っていく上で不可欠な、正当なビジネス情報交換の妨げとなり、ひいては経済成長および経済効率をも損なうこととなる。同様の理由から、公知の情報への同保護の拡大適用はほぼ無益である。

事業者の収集する個人情報、責任ある有益な方法で利用に供されるよう保証するという目的は、極めて重要で有意義である。プライバシー規制は、商業用途での適切なデータ利用を促進するとともに、プライバシーへの合理的な期待を保護するべきである。さらに、日本政府の支援する APEC プライバシーフレームワークに則り、プライバシー保護は、個人情報の収集、利用、開示により被る可能性のある被害のリスクおよびその重大性に見合ったものでなければならない。これら 2 つの概念は、あらゆるガイドライン等の策定の指針となるべきである。

## 2. 1 (2) いわゆる「過剰反応」について

要旨：規範的で矛盾の多い、または分かりにくいプライバシー規制は、事務・金銭上の多大な負担を生み、コンプライアンス、商業活動のいずれをも阻害する。個人情報の使用・不使用、その方法については、個人が選択できるようにしなければならない。共同利用者は、他の共同利用者およびその代理人の行為には責任を負う必要はなく、自分およびその代理人の行為のみに責任を負うべきである。

コメント：名簿を“開示すべき・するべきでない”と言った複数の事例からも明らかであるが、プライバシー保護と社会/学界/ビジネスのニーズのバランスを適切に保つことは容易ではない。名簿についての事例が示したのは、ある種の個人情報に対し、利用の全面禁止など必要以上に厳しいプライバシー規制を適用することにより、従来認められてきた個人情報の商業、学究活動、または社会活動に向けた利用が妨げられるということである。一例として、政府は、住民基本台帳に含まれる個人情報の商業目的での利用を禁止するのではなく、「電話禁止 (Do Not Call) リスト」や「セールス禁止 (Do Not Market) リスト」(アメリカにある電話・セールスを禁止するよう求める為に、個人等が登録するリスト) によって個人がそのような商業目的での利用をオプトアウトできるようにすべきである。そうすることで、個人が自身の個人情報の使用・不使用、その方法について選択でき、正当な商業活動への不必要な妨げや制限がなくなる。

さらに、プライバシー条項が詳細で規範的であるか関係省庁による明確化がされていないためそのように解釈されている場合ほど、事務的な負担や順守にかかるコストが膨らむ。コンプライアンスのためのコストが法外なものであれば、事業者による既存ビジネスの継続または新規ビジネスの立ち上げの妨げとなる。同様に、ガイドライン等の混乱や矛盾によっても、事業者はその規制の解釈に過度に慎重になり、正当な商業活動が妨げられることとなる。

例えば、第三者との個人情報の共有への規制に関し、政府の提案では、共同利用者は他の共同利用者およびその代理人の行為に責任を負うとしている。これによると、事業者が共同利用をする際には、委託契約において求められる責任と同様の責任を負わされることとなる。個人データの共同利用は現在、利用開始前にかかる共同利用について本人に通知することにより認められている。しかし、責任者の設置を義務付けながら、現在政府が提供しているのは委託に関

する監督責任についてのガイドライン等のみであり、共同利用者およびその代理人への監督責任については何の説明もない。共同利用者間での個人データの管理責任者が他の共同利用者をどう監督するかについては曖昧なままである。

ACCJとしては、共同利用の通知を行うのであれば、各共同利用者の責任は、共同利用に供される個人データの細目に関する各々の行為（代理人によるものを含む）のみに限定し、他の共同利用者およびその代理人の行為に対する責任を負わされるべきではないと考える。共同利用者が他の共同利用者の行為に連帯責任を負うべき理由は見当たらず、場合によっては、そのような連帯責任は不適當である。

ACCJは、今後とも継続して、所轄官庁に対し、共同利用者への監督責任に関する明確化、および共同利用者の代理人への監督義務についての立場の再考を求めていく。

### 3. 1 (3) 広報啓発について

要旨：必要以上の通知は国民を鈍感にするだけであるため、個人情報の盗難（なりすまし犯罪等）につながる可能性のある実質被害または損害の重大リスクがある場合にのみ、安全管理上の事故又は違反に関する通知が義務付けられるべきである。

コメント：収集される個人情報、その利用目的、収集・利用について本人がオプトアウトできるものとその方法、および情報の保護方法については、個人への周知が図られる必要がある。その反面、通知義務が頻度および内容について過度または必要以上になると、誰も通知を読まなくなってしまうため周知の目的は果たされない。

例えば、安全管理上の事故又は違反に関し、事故又は違反の都度通知が行われるとすると、それは逆効果である。金融庁を始めとするいくつかの省庁では、安全管理上の事故又は違反等があった場合、監督当局および本人への通知ならびに事実公表を義務付けている。その他の省庁も、そのような通知を「望ましい」としている。結果として、事業者は実際には、侵害の大きさ、関係する個人情報の性質、または不正利用のリスクにかかわらず、すべての安全管理上の事故又は違反を逐一報告・通知することとなる。事故または違反による実際のリスクにまったく関係のない通知は、人々に不必要に恐怖を与え混乱を起し、更に、将来的に損害から身を守るための手段を講じる必要のある通知に対し人々を鈍感にしてしまう。

従って、ACCJは、統一性、一貫性のある取組みを行うためには安全管理上の事故又は違反に関する通知には明確な国の基準が必要であると考え。通知は、個人情報の盗難（なりすまし犯罪）につながる可能性のある実質被害または損害の重大リスクがある場合にのみ行われるべきである。安全管理上の事故又は違反の発生後に作動する、通知を必要とする合理的かつ安定した判断事項を明確に示すことが目標である。個人への通知は、例えば、個人情報の盗難の被害者となる「重大リスク」がある場合に行われるべきである。安全管理上の事故又は違反の発生都度、その結果及ぼされる損害の重大リスクに関係なく通知が行われれば、数多くの人々にとって実質被害に関係のない通知が送られ、逆効果を招くことにほかならない。

さらに、通知義務は、安全管理上の事故又は違反により取得された個人情報と実際に個人情報の盗難につながる可能性のある場合にのみ発生するべきである。例えば、暗号化された情報を入手しても、キーがなければ他人には使いようがない。被害を受ける本人と事業者との何らかの関係、ならびにセキュリティ侵害の種類およびその及ぶ範囲をめぐる個々の状況によって通知手段は異なる。事業者は適当な時間内に、予測される侵害の性質および影響範囲を究明し、独自に十分な調査ができるようであればならない。また、警察当局が事件調査をしている場合、警察当局からの求めに応じ、本人への通知を遅らせることもできなくてはならない。

#### 4. 2 (1) 項目 1 日本の個人情報定義の国際的な整合性について

コメント：国際的な見方とほぼ一致した個人情報定義を有することは有用であるが、ACCJは、個人情報の性質やその利用目的に一致した保護を行うことがより重要な課題であると考え。第1項で述べたとおり、すべての個人情報を一様に取扱うことはない。特に、通常業務の維持に必要な、正当なビジネス情報交換を抑制することとなるため、公知の個人情報およびビジネス上の連絡先情報には、個人情報保護法の適用を受けるその他の情報に課される義務を課すべきではない。さらに、第5項で述べたとおり、センシティブ情報に関する格別の措置が必要か否かは、利用目的によって決められるべきである。

#### 5. 2. (1) 項目 2、格別の措置が講じられる個人情報の分野について

要旨：個人情報の分野によって格別の保護を行うのではなく、情報の利用目的に応じた保護を行うべきである。正当なビジネス活動を行う上でセンシティブ情報の使用は不可欠である。例えば、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の利用目的は、個人の同意を得て行う場合は、当該資金需要者の返済能力の調査のみに制限されるべきではない。

コメント：個人情報にかかる格別の措置は、保護対象となるデータ分野ではなく、その情報の利用目的に焦点を当てるべきであるとACCJは考える。センシティブおよび非センシティブ情報の収集は、雇用活動や金融サービス部門等、事業者の適正な機能に必要である。例えば、生命保険や健康保険の付保、障害者の受入、組合費の徴収および支払、配偶者手当の支給、医療機関や組合を通じたローン、ならびに、業種によっては従業員の身元調査を行うために、センシティブ情報の収集がビジネス上必要な場合もある。結果として、個人情報分野によって格別のプライバシー保護を行うことは、情報を保護するにあたりもっとも効率的な方法ではないかもしれない。むしろ、情報の利用目的に応じた保護を行うほうが理に適っている。

ACCJとしては、内閣府に対し、この問題への取組みを再考し、単に個人情報の特定分野に保護を包括的に適用するのではなく、情報の利用目的に焦点を当てるよう促していきたい。しかし、この目標を達成するのに新たな規制等は必要ないと考えている。特に金融分野に関しては、「金融分野における個人情報保護に関するガイドライン」が制定されるとともに、業法や監督指針において個人情報の管理態勢に関する条文が明記された。これにより、センシティブ情報の取り扱いなど個人情報保護法では規制されていなかった部分についても十分に規制がかかる状態になったと評価している。新たな規制等を導入する代わりに、事業者が煩雑なコンプライアンス義務を負うことなく、センシティブ情報の収集および利用を含む正当な活動を遂行でき

るよう、既存のガイドライン等を再考、改良すべきである。与信情報に適用されるガイドライン等がその代表例である<sup>1</sup>。与信業界に関する金融庁および経済産業省のガイドライン等は、個人信用情報機関による情報の利用を、資金需要者の返済能力調査の目的のみに制限している。たとえ本人の承諾を得た場合であっても、それ以外の使用はこの制限により禁止されるようである。このような制限は、プライバシー保護に不必要であるばかりでなく、ポートフォリオに基づく与信リスク評価、または過剰融資への懸念の低減を目的とした、より効果的な手法を編み出したり、本人の承諾のもと、商品やサービスを本人へ提供する などといった正当な商業目的での与信情報の利用を妨げる重大リスクをもたらすものである。

### 6. 3 (1) ① ガイドライン等のあり方について

コメント：上記第2項で述べたとおり、ACCJは政府に対し、個人情報共同利用への規制を明確にし、各共同利用者が他の共同利用者およびその代理人の行為には責任を負わず、自分およびその代理人の行為のみに責任を負うことを確認するよう御願います。

また、ガイドラインは省庁間で可能な限り一致させ、省庁別のガイドライン条項は、それがやむを得ない特定のビジネス分野にとどめられるべきであると考えます。共同管轄がある場合は、その実施プロセスにおいて省庁間の強力な連携が不可欠である。この場合、政府は統一見解を作成し、共同判断または決定を出す必要がある。現在のように省庁間の違いを見つけ出すのが事業者の責任であってはならない。

### 7. 3 (1) ③ 事業者の監督強化について

コメント：第2項で述べたとおり、事業者は、個人情報の取扱いを委託する場合、その委託先の監督義務を負うが、共同利用者およびその代理人の監督を義務付けられてはならないと考える。

### 8. 3 (3) ① 第1項目 安全管理措置の水準について

コメント：安全管理措置の水準については、事業形態、情報の内容、量などに応じて適切な水準がかわってくるものであり、一律に法律で適切な安全管理措置の水準を線引きできる性質のものではないと考える。現在、より厳格な規制が必要な分野については、安全管理措置として求められる水準が個別にガイドラインにて提示されているので、ガイドライン等の内容を社会環境の変化に応じて見直していくことでたりると思われる。

---

<sup>1</sup> 金融庁のガイドライン第13条第3項では、個人信用情報機関からの情報を、たとえ資金需要者がそれ以外の使用に同意した場合であっても、資金需要者の返済能力調査の目的のみに制限している。

### 9. 3. (3)① 第2・3項目 事業者が直面するリスクを踏まえた安全管理措置を講じる必要性、および中・小規模事業者が情報セキュリティ対策整備に十分な費用や人員を有さないという懸念について

要旨：最適と思われる対応・手段を法律およびガイドライン等にて成文化するのは避けるべきであり、限定的で詳細なセキュリティ義務を定めるべきではない。個別環境を鑑みて、事業者が既存のセキュリティプログラムの拡張により個人情報保護への対応を図るよう促すことが、より一層個人情報保護の強化につながるであろう。

コメント：安全管理措置は事業者個別に調整されるべきであり、事業者ごとに取扱う情報の性質を考慮する必要があるのはもつともであると考え。保護対策は損害の見込および重大性、情報の機密性ならびにその内容に見合ったものでなければならない。セキュリティ要件は法規制において大まかに規定されるべきであり、限定的で詳細なセキュリティ義務があってはならない。事業者は、その時点において最新のものを、導入コストを鑑みて考慮できるようにしなければならない。

「ベストプラクティス」を法律およびガイドライン等にて成文化するのは避けるべきである。さもなければ、顧客の個別要求に対応し、費用効率の高い解決策を選択し、新規アプローチを開発、導入するビジネスの柔軟性が制限されてしまう。さらに、事業者の多くが既に秘密情報および企業秘密の確実な保護システムを有しており、そのような事業者には、まったく新しい基盤構築を求めるのではなく、既存のシステムを拡張した個人情報保護への対応を認めるべきである。事業者に対し、その個別環境において、既存のセキュリティプログラムの拡張により個人情報保護への対応を図るよう促すことこそがより一層個人情報保護の強化につながるであろう。

つまり中小企業については、ガイドライン等に定める特定の手法に従わせるのではなく、既存のセキュリティプログラムの拡張による個人情報保護対応を認めることで、費用対効果の高い形で情報セキュリティ対策を強化することができるであろう。

### 10. 3 (3) ②安全管理と労務管理について

要旨：ガイドライン等が定める、完全な新規データベースの作成・維持を必要とする「個人データ取扱台帳」などの過剰に詳細な安全管理要件は、多大な労働力と経費を必要とする。そのため、費用対効果が高く統一の取れた最先端のセキュリティプログラムを、全世界的規模で考えるという全体的な企業努力を損なうものである。

コメント：上記で述べたとおり、ACCJは、原則として、安全管理措置は事業者向けに個別に調整されるべきであり、法が定める安全管理要件は大局的に記述し、具体的かつ詳細な安全管理義務を含むべきではないと考える。よって、ACCJは、既存のガイドライン等に記載された安全管理に関する条項が、不必要に具体的かつ詳細であると考え。さらに、個々の安全管理規

定とその強制または任意の度合いは、ガイドラインにより大きく異なっている。この結果、順守にかかる負担は、特に複数のガイドラインを順守しなければならない事業者の場合は莫大なものとなり得るため、費用効率が良く、統一の取れた最先端の安全プログラムを全世界的規模で考えるという全社的な企業努力を損なうものである。

経済産業省と金融庁などが定める「個人データ取扱台帳」が、上記の一例である。安全管理措置の一環として、経済産業省と金融庁のガイドラインは、個人情報の取扱い方を確認できる措置の実施を要件としている。経済産業省のガイドラインは、この要件を順守するために、当該台帳に記録しなければならない様々な情報（取得項目、利用目的、保管場所、保管方法、アクセス権限を有する者など）の категорияについての例を挙げて、「個人データ取扱台帳」を作成することを「望ましい」としている。しかしながら、金融庁の安全管理措置は、当該個人データ取扱台帳を作成することを義務付け、かつ、その台帳に、情報の様々なカテゴリー（取得項目、利用目的、保管場所、保管方法および保管期限、管理部署、アクセス制御の状況など）を含めることを義務付けている。さらに、この個人データ取扱台帳を「定期的に」点検し、常に更新することを義務付けている。かかる情報を含む完全な新規データベースを作成するには、多大な労働力と経費を要するうえ、ガイドライン等によりこれらの措置が強制か任意かの別が異なっているため、コンプライアンスの度合いが異なる状況を生んでいる。上記第9項で述べたとおり、企業に対し、その個別環境において、既存のセキュリティプログラムの拡張により個人情報保護への対応を図るよう促した場合には、個人情報保護の強化につながるものと考えられる。

### 11. 3 (3) ③委託先の監督について

コメント：事業を遂行する上で、業務の委託や委託先の変更は頻繁に多く行われることであるため、委託先を消費者等に何らかの方法で周知・告知しなければならなくなった場合には、事業の運営が困難となり、事業者にとっての負担が著しく大きい。また、委託先の数は膨大であるため、それを公表しても消費者にとって有意義な情報になるとは思い難い。現行法上、委託元は、委託先を管理監督する義務を負っており、それに基づき委託先において安全管理措置が講じられる状態になっているので、委託先の透明化は必要ないと考える。

### 12. 3 (4) 第三者提供の制限について - M&A プロセスにおける個人情報の移転について

**概要：**企業秘密などのきわめてセンシティブなその他の情報は、通常、Mergers & Acquisition（“M&A” = 企業買収）において、秘密保持契約を締結した上で提供および保護されるため、M&Aにおける個人情報の第三者提供について同意を得る義務の免除は、デューデリジェンス（企業買収における調査）のプロセスにおいても適用されるべきである。

コメント： ACCJ は日本政府に対し、合併または買収における個人情報の利用について、現行の個人情報保護法およびガイドライン等の解釈を見直すよう繰り返し強く要請してきた。合併や買収の初期段階でのデューデリジェンスの手続きにおける個人情報の提供に係る制限は、

非現実的で、日本における M&A 活動を妨げるものである。デューディリジェンスは、M&A の通常業務において必要なプロセスであり、取引の査定を目的として、通常、当該取引を企図する当事者間で、企業秘密を含むきわめてセンシティブな情報が提供される。

上記にもかかわらず、個人情報保護法により当該要件が免除されるケースは、合併、買収または分社化の完了後に個人情報が移転する場合に限られている。この免除は、デューディリジェンスが行われている間の情報提供には適用されない。経済産業省は、個人情報が匿名化されるか或いは本人のオプトアウトがない限り、デューディリジェンスのプロセス中にも該当する個人全員の同意を得るべきであるという立場を取っている。身元が判明しやすい顧客または従業員の情報が懸案中の取引の査定に必要な案件によっては、匿名化やオプトアウトが不可能な場合もある。例えば、投資予定者や事業買収予定者は、上級管理職に対し同等の報酬を支払えるか否かを判断したり、合併後に新会社が従業員を追加雇用する必要があるか否かを判断するために、上級管理職に提供されている報酬体系の情報を要請する場合がある。このように、政府の取組みは非現実的であり、インサイダー取引のリスクを高めるものである。一般的にデューディリジェンスの前に非開示契約を締結することで、取引が最終的に成立しなかった場合にはこの非開示契約に基づき、買収予定者は受領した個人情報のすべてを返却または破棄する義務を負うので、個人の利益の保護が可能である。

### 3(4) 第三者提供の制限について

コメント：個人データの取扱いの委託の場合には、「利用目的の達成に必要な範囲に限り」個人情報を第三者に提供できることとなっており、利用者の範囲は十分に限定されていると考える。また、合併の場合には事業を継承しているので、継承前の利用目的で利用できるのは当然のことであり、現行法以上に利用範囲を狭める必要性はないと思われる。

### 13. 3 (5) ① 事業者が定める利用目的について

**概要：**与信報告目的または個人情報の取り扱いを委託する場合など限られた例外を除き個人の同意を得ることを条件として、企業が個人情報を収集し、利用することが可能となるべきである。通知要件は、十分な情報提供と過剰な詳細情報との間のバランスを保つべきであり、さもなくば、個人は通知を読まなくなるものとする。

コメント：第3項で述べたとおり、個人は、どのような個人情報が収集されているのか、その情報の利用目的、収集・利用について本人がオプトアウトできるものとその方法、および情報の保護方法について通知されるべきである。また、第5項で述べたとおり、個人の同意を得れば、企業は個人情報を収集し利用することができるはずである（返済能力に関する情報を含めて）。利用目的についての個人の同意は、顧客が当該利用目的を開示する契約を締結した時点で存在するものとみなすべきである。また、一定の制限つきで、オプトアウトが認められるべきである。とりわけ、顧客が契約したサービスや製品の提供と合理的な関連がない目的で情報が利用される場合には、オプトアウトが認められるべきである。たとえば、ローン商品に関連して得られた情報をマーケティング目的で利用することについて同意した顧客には、マーケティング目的が当該ローンサービスの中核目的ではないという理由で、後日オプトアウトを行うことが認められるべきである。とはいえ、個人情報が与信報告目的で提供されたり、メール送

信業者やデータ処理業者など個人情報の取扱いが委託される場合にはオプトアウトは認められるべきではない。

通知により利用目的についての十分な詳細が提供されるとともに、その利用目的に変更がある場合はいつでも通知するべきである一方、利用目的を詳述することについて過剰な通知義務を課すことは、個人に情報提供する目的の達成を意味しない。事業者に対して個々の利用目的すべての列挙を義務付けることにより、通知は過剰に詳細なものとなり、その頻度が非常に高くなる。いずれのシナリオにおいても、個人の大半は、単に通知を読まなくなるものとする。さらに、個人に対して繰り返し通知し、同意を得ることは、事業者にとっては極端にコストと時間がかかり、事業者に対しても個人に対しても、何ら利益を生むものではない。バランスを取るべきことは明らかであり、事業者は、その事業セクター・産業セクターに関する通知について、最も相応しい内容・頻度を判断するための指針を与えられるべきである。

また、顧客情報をどのように利用するかは、事業戦略によって異なるため、定款又は寄付行為に記載された事業を全て揚げるのが一概に「利用目的をできる限り特定していないこと」にならないと考える。事業者は、利用目的ごとに個人情報を管理する必要があるため、個々の取引ごとに利用目的を個別に設定していくことには個人情報の管理上限界がある。利用目的を広くとったとしても、利用目的が特定されていけばよいのではないかと考える。

#### 14. 3 (5) ② 個人情報の取得元の開示について

コメント：個人情報の種類、内容、取得経緯等によって、個人情報の取得元は異なるため、取得元の情報は、ホームページなどにより全消費者を対象に一律に公表できる性質のものではないと思われる。また、個々の個人情報ごとに、取得元の情報を管理しなくなればなくなった場合、「個人情報ごとに取得元が異なるケース」、「1つの個人情報を複数の取得元から取得しているケース」等に対応するために膨大なシステム対応等が必要となり、かつ、事業者への負荷も大きく、事業運営に支障をきたす場合もあるため、事業者取得元の情報を管理させることについては慎重な検討が必要である。

#### 15. 3 (5) ③ 個人情報の利用停止・消去について

コメント：日本政府は、データの消去は法令が求める法律上の保管期限に従うべきことを明確化するべきである。とりわけ、事業者が法律上の理由や合法的な事業目的でデータを保管する必要がある場合には、そのような情報の消去が強制されるべきではない。例えば、米国の会社の日本の子会社の場合、米国の親会社が召喚を受けているデータを保管する必要がある場合がある。この場合、当該データを保管することは、日本の法的要件とは相反するものの、社内ポリシーに基づく義務であると考えられる。同様に金融業界や不動産業界においても、顧客との取引履歴を管理・保管する必要があるため、本人の求めがありさえすれば個人情報を消去することを義務付けることは適切ではない。従って、法的要件、事業者における情報の必要性および本人の利益を考慮して、適切なバランスを保つ必要があると考える。

## 16. 5 国際的な整合性

**要旨：**ガイドラインの全条項は、APECの責任の原則に準拠すべきで、責任とデータの第三者移転に係る同意取得の両方を要求している経済産業省のガイドライン第5条がAPECの原則から逸脱している例としてあげられる。日本は、事業者が「企業プライバシー規則」または行動規範を確立することを認め、事業者がその組織内で個人情報に全世界的にアクセスし、利用するための統一のアプローチを策定し、これを実施することができるようにするべきである。

**コメント：**データの流通が国際的であることや、国際的な事業者がデータを世界中に送信する必要があることに鑑み、責任要件にデータの国内移転と国外移転との区別を定めないことが、最も理にかなっており、論理的なアプローチである。グローバルなネットワーク経済の時代において、情報の伝達は、もはや整然と確立した経路に従うものではない。むしろ消費者ニーズやビジネスニーズを満たすにあたり、情報は数多くのチャンネル（インターネット、電子メール、集中管理されたデータベース）を介する複数のチャンネルを介して企業内の世界中の人員に伝達される。多くの諸国が、データの国外移転に対する制限規則を定めているが、その規則が商取引に悪影響を与え、グローバルな事業者がその事業を費用対効果の高い能率的な方法で経営する能力を妨げることも考えられる。

国際的なデータの流通に関する問題を取り上げるとともに、この地域における情報のプライバシー保護に向けての首尾一貫した取組みを促進するために、日本政府は20カ国以上の諸外国と協力して、2004年にAPECプライバシー・フレームワークを策定し、これを承認した。APECプライバシー・フレームワークにより、従前の国際的なデータ流通のプライバシーに関する取組み（世界中のプライバシーに関する法律、とりわけヨーロッパ諸国の法律の多くにみられる、個人情報の収集、保有、加工または利用を管理する組織に対して(a)情報が所在地を問わない第三者に伝達された場合にも、当該情報の保護について引き続き責任を負うか、(b)本人から同意を得るかのいずれかを義務付ける方法）は使われなくなった。<sup>2</sup>この責任の原則は、事業者がその組織内でグローバルに個人情報にアクセスし、これを利用することに対する統一のアプローチを策定し、これを実施することができるようにすることを意図するものである。

APECの加盟国が現在直面している課題は、それぞれの経済圏でAPEC原則を実施し、企業グローバル・プライバシー規則・行動規範などのメカニズム、個人情報取扱いに関する社内のポリシーもしくは手続きまたは契約上の取決め、これにより事業者がその組織内で個人情報にグローバルにアクセスし、利用するための統一のアプローチを策定し、実施することができるように

---

<sup>2</sup> EUは、過去数年にわたり、モデル契約条項の活用を促進するなどして、EUデータ保護条令により生じる国際的なデータ移転の障害の問題に取り組んできたがあまり成果をあげていない。最近になって、オーストリア、フランス、ドイツ、ハンガリー、アイルランド、オランダ、ポーランドおよび英国のデータ保護に関する検査官が、行動規範または彼らが好んで呼ぶところの「拘束力ある企業規則」（“Binding Corporate Rules”）の使用を推進のための協力を始め、EUがデータを移転できるようにすべく取り組んでいる。ただし、規制に関する許認可を得るための能率的なメカニズムがないことが、ヨーロッパ内でこの活動を広く浸透させるための障害のひとつとなっている。

なるものを承認し、認知するため、地域ごとに能率的な取組みを確立するべく協力することである。

データの流通が、国内・国際間を合理的に区別する方法はない。実際のところ、事業者は、一貫性のあるプライバシーポリシーを地域の枠を越えて世界中で実施することができるため、プライバシーに関するコンプライアンスが高まり、プライバシー保護が強化されると考える。従って、情報の移転や開示について、組織の内外の区別や、国内・国際間の区別は、重要ではない。<sup>3</sup>

とりわけ、「企業プライバシー規則」は、国際間の個人データの流通を保護し、国際的なプライバシー保護を促進するための最も有望な方法のひとつである。企業プライバシー規則により、消費者の個人情報保護の統一水準に相応のものであることを確保し、複数国における特にオンライン取引に関するデータ処理活動に適用される法的制度を定める必要をなくして、現地で請願メカニズムを提供することができ、また、国際的なデータ移転についてのプライバシーの順守にかかるコストを簡素化するとともに低減させることにより、コンプライアンスの高まりを助長することができる。

従って、日本は、可能な限りいつでも、事業者が個人情報を収集、利用および開示するにあたり適用できる企業プライバシー規則または行動規範を確立することを認めるべきである。複数国におけるデータ処理活動について単一の規則が適用されることにより、法的制度を定める際の不透明な状態から生じる困難が軽減されるものとする。例えば、韓国に事務所を有する事業者が、日本の顧客から情報を収集し、その処理のためにオーストラリアにデータを移転する場合、どの法律が適用されるのかを確認するのは相当困難である。これら異なる法域の規則は、相矛盾する法的要件を定めている場合があるため、不必要に複雑で場合によっては解決不可能なコンプライアンスの負担を生じさせ、個人にとって、負担に見合う利益または確実な利益が得られない場合がある。実際、いくつかの異なる制度を適用し、その結果生じる複雑な問題およびコストにより、コンプライアンスに向けての努力を減退させ、プライバシー保護の高い水準が損なわれる可能性さえあると考える。

企業プライバシー規則の策定を促進する第1段階として、日本政府は、すべての省庁のガイドライン等をAPECの責任の原則に準拠するものとするよう確実に期すべきである。とりわけ、経済産業省のガイドラインの第5条は、事業者が、その事業者となんら関係のない第三者に対して個人情報が移転された場合に、当該情報の移転が本人の同意を得た上でなされたものであっても引き続き責任を負うことを示唆しているという点で、当該原則から逸脱している。OECDプライバシー・ガイドライン、EUデータ保護条令その他の世界中のデータ保護に関する法律の要件を超える要件は、国際的なデータ移転についてのグローバルな解決策の整備を妨げるものだと考える。

---

<sup>3</sup> プライバシーに関して、国内のデータ移転と国際的なデータ移転を区別しない法律を採択しているのは、日本とカナダだけである。

#### 17. 6 (1) 独立のデータ保護機関の必要性について

コメント：現在の規制システムにおいては、12もの省庁が、各セクターのコンプライアンスについて監督している。事業活動の範囲を考えると、多くの事業者が、複数の省庁の規制監督下にある。さらにプライバシー保護を管轄する別の機関を既存の規制当局に加えると、既に存在している管轄当局の重複はさらに広がり、これにより、混乱や過剰な規制が増し、既に事業者が抱えている重いコンプライアンスの負担が増大するものと考ええる。

#### 18. 6 (2) 現行法は生存する個人に関する情報のみを保護の対象としていることについて、どのように考えるか。

コメント：保護すべき対象がない中で規制をかけることは難しいので、死者の情報を保護の対象とする場合には、誰にどのような権利を付与するかについて慎重な検討が必要である。