

断に利用するか否かにかかわらず、保護の対象とするべきである。ただし、その場合であっても、一般的な預金情報については、その漏洩等は罰則の対象とする一方、後述するように、収集に当たって事前同意を要しないこととするなど、保護の在り方には現実的な対応も必要である。

- (12) また、証券取引において、適合性の原則（注5）に則して業務を行うために、顧客の資産等について情報収集を行うことがあり、その他の金融商品の販売に関しても、様々な個人情報が収集されている。証券取引における適合性の原則は、投資者の観点から行われる規制の一類型である。証券取引や金融商品の販売に関して得られた情報は、現在は断片的に担当者や店舗に蓄積されるに止まっているものの、今後、金融システム改革の進展、金融商品のさらなる多様化などに応じ、これらの情報の重要性は一層増大していくことになる。したがって、このような金融取引に係る情報についても、今後の収集・利用の状況によっては保護を検討していくことが考えられる。その場合には、この報告書で検討されている個人情報保護の保護基準が当てはまると思われる。

（注5）適合性の原則の例（証券取引法第54条抜粋）

「有価証券の買付け若しくは売付け又はその委託について、顧客の知識、経験及び財産の状況に照らして不相当と認められる勧誘を行って投資者の保護に欠けることとなっており、又は欠けることとなるおそれがある場合」には、大蔵大臣は監督上必要な事項を命じることができる」とされている。

- (13) 電子商取引についても、決済に関する情報が決済サービス提供者に集積され得るが、具体的なスキームごとに、集積され得る利用者の個人情報の程度や範囲は異なる。電子マネー・電子決済の利用に伴う個人情報の取扱いについては、利用者にとって重要な個人情報の集積を行うこと、集積された個人情報の利用範囲等について適正な管理や利用者の同意が行われること等が必要である。ただし、こうした決済に関する個人情報の取扱いについて法規制を考える場合には、電子商取引や取引一般に係る個人情報全般をどのように取扱うべきかといった議論に留意する必要があり、具体的な制度整備の段階において、その進捗状況を展望しつつ検討していく必要がある。

2. 行為規制の対象者の範囲

- (1) 個人情報保護の保護に当たっては、個人情報の範囲を明確にするとともに、それを収集・利用するものに対して、法的措置や自主ルール等により重層的に措置を講じることが適当であると考えられる。
- (2) 行為規制の対象は、行為として与信という領域の中で情報の集積・交換を行うという特殊な性格を有する信用情報機関及びこれら機関と情報交流を行う与信業

者に限定すべきとの意見もあったが、漏洩等の実態からより広く、業務として個人信用情報を組織的に取り扱うものを一般的に取り込むべきとの考え方が大勢であった。

- (3) 業務として個人信用情報を組織的に取り扱うものとしては、信用情報機関（定義は後述）、業として与信を行う与信業者（銀行・保険会社等の金融機関、貸金業者、クレジットカード会社、割賦販売業者等）、及びこれらに係わる与信業者に準ずるものとして保証会社（注6）、債権回収代行組合等が考えられる。なお、この点に関して、割賦販売業者のうち自社割賦のみを行う業者まで対象にする必要があるのかという意見や、主として事業法人を顧客としているリース業者等は必要がないといった意見があった。

（注6）保証会社

消費者ローン、住宅ローン等に債務不履行が生じた場合、これらのローンを提供した金融機関に対して保証を行う機関の総称で、主に金融機関が出資母体となっている。業務としては、金融機関と保証契約を締結し、債務者の不履行に伴い金融機関に対し代位弁済を行った上で、自らが回収にあたる。

- (4) また、情報の漏洩の防止の観点から、上記のような機関、業者から情報提供を受けるもの（業務委託先、その他債権譲渡先、グループ企業等）に対して、また、情報の正確性の確保を図る観点から、信用情報機関に情報提供を行うもの（例えば不払い情報を提供する電話会社、通信販売業者等）に対しても一定の行為規制の対象とする必要があるだろう。

3. 情報の収集等に当たっての本人の同意と収集の制限

- (1) 個人信用情報の収集に当たっては、契約の履行のために必要な場合やデータの処理を外部に委託する場合等一定の場合を除き、情報主体の明示の同意を要する（収集制限の原則）。また、情報主体に対し、事前に①利用目的、②管理責任者名、③情報主体の権利、④第三者に提供する場合には提供先・提供目的などを知らせなければならない（目的明確化の原則）。
- (2) 金融機関の場合には、1(1)で論じたように、与信業務と無関係に預金情報を収集している。預金情報の収集の際には、与信判断に利用され得ることについて同意は要しないが、金融機関部内で当該個人への与信の判断のために利用するような場合には、原則に戻って改めて同意を得るべきである。金融機関が預金業務で得た情報を自社のダイレクトメール発送に利用するようなことも考えられるが、本人の意思に反したダイレクトメール発送の中止を求めることができる点が確保されれば、このような利用について事前の同意を不要とすることは容認し得るものと考えられる。

- (3) 与信業者がグループ内の与信業者でない会社などから、事前に情報主体の同意を得ていない個人信用情報を間接的に、与信判断に利用する目的で入手する場合などにも改めて情報主体の同意をとるべきである。
- (4) 与信契約の締結やその履行に関して情報収集を行う場合、情報主体としては、情報を提供しなければ与信を受けられない等の不利な立場にあることから、バーゲニングパワー是正のための措置が必要である。具体的には、以下のようなものが考えられる。
- ① 同意は文書によるものとし、口頭による補足説明を行うことが望ましい。郵送による申込みである場合においても、十分な説明の確保が図られるようにする。
 - ② 与信申込み時に与信判断に関係しない情報や当該契約に関係しない情報の提供は、任意である旨の説明を行わなければならない。また、任意に求める情報は、申込書等で与信判断のために必要な情報と明確に区分し、任意である旨明示した上で提供を求めることとすべきである。
 - ③ 与信判断目的以外の利用については、自己情報の利用提供を拒絶できることとする。
- (5) ハイリーセンシティブ情報（国籍、信教、政治的見解、保健医療、犯歴等個人の機微に深く関わる情報）や本人識別情報でプライバシーの侵害のおそれがある情報（戸籍等）の収集・蓄積は、与信目的であっても、原則として禁止し、収集がやむをえないと考えられる合理的根拠がある場合で、かつ本人の明示的方法による承諾がある場合に限って認められるものとすべきである。また、これらの目的外の転用、外部への提供は一切禁止すべきである。この際、合理的根拠がある場合とは、労働金庫から与信を受ける場合に組合員資格を問われる等、ハイリーセンシティブ情報自体が融資の条件となっている場合に限定すべきである。

4. 情報主体（消費者）の個人信用情報に対する権利

- (1) 情報主体の権利には、以下のようなものが含まれる。これらの権利行使を円滑にするため、契約締結時に書面に明記するなど手続きを明確化しておくことが必要と考えられる（個人参加の原則）。
- ① 開示請求権（自己の個人信用情報を保有しているかどうかについて確認を求めるとともに、保有されている情報の内容、目的、情報源、提供先等を自己に開示するよう求める権利）
 - ② 誤情報の訂正の請求権（保有されている自己の個人信用情報に誤りがある場合に、その誤りの訂正及び情報提供先等への訂正通知を求める権利）
 - ③ 異議申立権（本人の意思に反して情報が利用等されることを防止するため、同

意のない自己情報の利用、販売促進等を目的とした利用・提供、情報の電算処理等一定の場合を除く外部への提供に対して異議申立を行う権利)

- (2) 開示手続きにおいて、本人以外に開示すると損害賠償を求められるとのおそれから本人確認を厳格に行いすぎると、開示を事実上制限することとなるため、一定の書面において本人を確認した場合には免責されるようにすることも検討すべきである。
- (3) 訂正を請求する場合には、書面により明確な理由を付すこととし、それに対し与信業者や情報機関は調査する義務を負うものとするのが適当である。なお、最後まで誤情報かどうかの確認がとれなかった場合、信用情報機関においては、その旨コメントを付して再登録を行うことも考えられる。
- (4) 情報主体から情報の利用・提供に対して異議申立があった場合、契約履行のために必要な場合、事前の同意に基づく与信判断目的の利用の場合、公共の利益のため法令で求められる場合を除き、これに応じなければならない。

5. 本人以外による情報の開示請求

- (1) 情報の開示対象は原則本人のみとすべきである。しかしながら、多重債務問題の現状にかんがみると、本人と同一の責任を負う連帯保証人への開示、本人が失踪している場合や本人が貸出禁止依頼をしている場合に限って、同居配偶者・親子・兄弟姉妹への開示も認めるべきであるとの意見があった。また、将来、成年後見人制度が整備された場合には、後見人への開示も認めるべきとの意見もあった。
- (2) 公共の利益のために行われる開示については、まず、令状に基づく捜査、監督官庁による立入り検査等開示を行うことが法的に強制される場合には当然開示が必要である。捜査照会に対しては、現状では信用情報機関等の対応にバラツキがみられるが、統一的なルールにより対応が図られるべきである。捜査照会（刑事訴訟法第197条第2項に基づく照会）を受けて応じた団体等は、これにより故なく秘密を漏らしたことになることはもちろんであるが、それにとどまらず、捜査照会には応じて捜査に協力すべきであることから、取引先の名称等について、この趣旨に沿って必要な対応がとられるべきである。
- (3) 債務者のためのカウンセリングは本人の利益にもかなうものであるが、カウンセリング機関が相談者の債務状況等のチェックを勝手に行うべきではない。一方債務者本人への便宜も考慮すると、債務者が信用情報機関の開示窓口に出向かなくとも、カウンセリング機関において本人が信用情報機関から開示を受けられるよう、カウンセリング機関と信用情報機関の間にオンライン回線、利用端末等が

設けられることが望ましい。

6. 情報の適正管理

ア. 安全保護措置

- (1) 個人信用情報の漏洩、目的外利用等を防止するため、安全保護措置として、管理責任者の設置、社内教育の徹底及び従業員の守秘義務を就業規則に定める等の管理面の保護措置とともに、アクセスにはIDカード等を要することとし、アクセスに当たっての暗号（パスワード）を適切に管理しなければならないこととするなど、技術面での保護措置が十分でなければならない。また、与信業者や信用情報機関自体による内部監査は必須である。例えば、与信業者においては、与信業者の従業員による信用情報機関の情報の不正利用を防止するため、与信申込み件数と信用情報機関への照会件数を照合する方法がある（安全保護の原則）。
- (2) 個人信用情報をコンピューター管理したり、顧客リストのように容易に検索し得る形で管理する場合、これらのデータベースに誰でもアクセスできるとなると、大量かつ簡単に漏洩等が起こるおそれがある。こうした方式を採用する場合には、厳重な管理が必要である。例えば情報管理責任者はデータベースにアクセスできる者を選定し、この者以外のアクセスを防止する等の措置がとられる必要がある。
- (3) 与信業者が多様な分野に事業展開を行っている場合には、同一企業内における他部門の利用を制限するなど、情報の適正管理のための措置が特に重要である。
- (4) コンピューターやネットワークを介する場合、たとえ漏洩等が生じても容易にその事実が判明しないことが予想される。このため、データベースにアクセスしにくくすることは当然のこととして、データへのアクセス記録を残すなどの措置も必要である。ネットワーク犯罪については捜査が困難との指摘があり、こうした措置が事案解明にも役立つものと考えられる。

イ. 最新性・正確性の確保

- (1) 古い情報は誤情報となるおそれ大きいことも踏まえ、情報の最新性・正確性を確保する観点から、現在信用情報機関においては5～7年で個人信用情報を保有する期間を限定しているが、与信業者においても保有する期間を限定すべきである（データの質維持の原則）。
- (2) 同姓同名等によるトラブルを防止するため、信用情報機関への登録・照会に当たっては、氏名・生年月日だけではなく、住所等で本人確認を厳格に行うべきである。

ウ. 外部委託先等への情報提供

- (1) コンピューター処理や書類の破棄等について外部委託が行われることが多い今日、委託先から漏洩等が生じる可能性は高い。しかしながら、実務上の便宜を考

慮すると、独立して情報を利用しない委託先への情報の提供は同意を要しないとすることもやむを得ないと思われる。ただし、与信業者等一次的な情報収集者は委託先の守秘義務、再提供・不正蓄積・目的外利用の禁止、事故時の責任分担などを委託先との委託契約に定めるとともに、情報主体との契約等により外部委託に伴う委託者の責任も明確にしなければならない。この際、情報主体との間で契約等により責任を明確にせず、外部委託により情報主体が損害を被った場合には、委託者も責任を負うこととするなど、契約適正化のための措置も必要である。

- (2) その他の第三者への提供は、書面等による同意の範囲内での提供に限られるべきである（利用制限の原則）。また、提供先が直接に情報保護について責任を持たなければならない。さらに、情報の拡散により漏洩等の危険性が拡大すること、情報主体のコントロールが及ばなくなること等を考えると、情報を受けた委託先を含む第三者からの再提供は行わないこととすべきである。真に再提供が必要な場合には、与信業者が情報の取り扱いについて直接情報提供先をコントロールできるようにしておくべきである。
- (3) なお、その他の第三者への提供前の時点で、情報主体から自己情報の利用の中止を求められた場合には、情報主体に中止する機会が与えられている旨、情報主体との契約書で明らかにしておくべきである。

7. 個人信用情報漏洩等の早期発見とその抑止

- (1) 情報の特質として、容易に複写、伝搬が可能であるため、実際に漏洩等が起こった場合においても、証拠等が残らない可能性が高いという点がある。したがって漏洩等を早く発見し、早期に必要な措置をとることが重要である。
- (2) 情報主体としては、不必要な情報を提供しないことや、提供した情報がどのように取り扱われているか契約書をチェックする等、慎重な対応が必要であり、適切に開示を求め、誤った情報は直ちに訂正させるなど、アクセス権を行使し、自己防衛する姿勢も重要である。また、これら情報主体の情報保護に関する認識の必要性、アクセス権等情報主体の権利やその権利行使の重要性については、消費者教育等を通じ、啓発を図っていくべきである。
- (3) 第一義的には本人が容易にアクセス権を行使できるような環境の確保が必要である。すなわち情報主体自身が、誰がどのような情報を保有し、どのように使っているのか確認することができるようにする必要がある。また、情報を収集するものとしても自分が情報を受け取ってよいものか確認できることが好ましい。このため、与信業者等は保有する個人信用情報の項目等を公開し、誰でも閲覧できるようにしておく必要がある（公開の原則）ことから、行政機関への届出書類を一般閲覧に供することも一案である。

(4) 与信業者が会員となっている信用情報機関の情報については、信用情報機関自身によるモニタリングが有効である。例えば、登録情報数と照会件数を比較するといった方法により、与信業者が適切に情報登録しているか、情報の不正使用等をしていないかを系統的にチェックすることが効果的であり、必要な場合には立入検査を実施し、不正の防止に努めるべきである。また、消費者からのクレームがあった場合、例えば、誤情報が登録されているとのクレームに対しては、信用情報機関が与信業者に調査報告を求めることも可能とすべきである。このような信用情報機関によるモニタリング機能の重要性にかんがみると、これらの機関を登録制とするなどにより公益的性格を付与することが望ましいとの意見があった。

8. 民事訴訟手続きによる救済

個人信用情報の漏洩等が起きた場合には、民事訴訟手続きに基づき、不法行為に対する損害賠償のほか、情報の利用・提供の差止や情報ファイルの破棄といった原状回復措置がとられることが必要である。この際、情報主体が漏洩等のプロセスを全て立証することは困難であり、挙証責任の転換が必要という意見があった。

9. 行政機関による監督

(1) 消費者が裁判所に民事訴訟手続きによる救済を求めることは、実際にはコストと手間を考えると困難な場合が多い。したがって、行政機関が消費者に代わって個人信用情報の漏洩等の防止と救済を図ることも有効であると考えられる。具体的には、①与信業者等の行為規制対象者に情報収集項目等の届出をさせること、②立入検査・報告徴収を行うこと、③漏洩、不正使用、情報の不開示や情報利用の拒絶に応じないといった行為義務違反への処分、④不正取得や不正使用・蓄積を行っている者への行為の中止命令、さらには⑤ID、暗号（パスワード）によるアクセス管理を怠るなど不適切な情報管理を行っている業者への是正命令や勧告等も考えられる。

(2) なお、行政機関の監督の在り方や監督官庁については、行為規制の対象者の性格や行為規制の内容により、具体的な対応を変えることが求められる。諸外国においては、データ保護を担当する専門の機関、例えば英国等のデータ保護登録官やオーストラリアのプライバシー・コミッショナーのようなものを設けている例もみられる。個人信用情報に限定した立法を行う場合、当面は個人信用の与信を行う業者を所管する官庁が監督するとしても、将来的には、諸外国の例にあるような専門の機関についても検討してはどうかとの意見があった。

- (3) 後述するように、信用情報機関については、その公益的役割にかんがみ、登録制等とすることも考えられる。

10. 刑罰の適用等

- (1) 個人信用情報の漏洩事件が数多く発生していることや、情報保有者が情報管理を適切に行っていたとしても、外部のものの侵害行為を完全には防止することができないことから、刑罰の適用により個人信用情報の漏洩、不正取得等の抑止を図ることが必要であると考えられる。情報主体と契約関係にある場合には、契約に基づくコントロールが可能であるが、契約関係にない第三者の侵害行為については、刑罰による抑止以外には特段有効な手段がない。
- (2) 刑罰の適用を考える場合、現状では個人情報一般について、その侵害行為が刑罰の対象とされているわけではないこととのバランスや、また、補充性の原則（他の手段で抑止が可能であれば、まず、それを用い、刑罰は補充的に用いるとの考え方）を考慮する必要がある。したがって、刑罰適用による保護の対象としては、個人信用情報の全てとするのは適当ではなく、ハイリーセンシティブ情報や信用判断に直結する情報等重要な情報に限定すべきであるとも考えられる。実際に情報漏洩、不正取得等が生じる場合には、通常これら重要な情報も含まれていることから、処罰の適用対象を限ったとしても問題解決に不都合は生じないものと考えられる。他方、情報の内容・種類による区別は困難であり、与信業者等が収集・保有する個人信用情報を全て対象とすべきという意見もあった。なお、刑罰の対象とならないものについても、行政罰等により担保措置を講じることは必要である。
- (3) 情報保有者による不正行為としては、情報の漏洩、不正提供、不正利用があるが、これらに対し刑罰を科す必要がある。場合によっては、いわゆる両罰規定によって法人に対しても刑罰（罰金）、業務停止等の行政処分を課すことも考えられよう。なお、最近の事件の実態を見ると、内部の従業員や元従業員が無断で不正提供、不正利用を行うケースが一般的である。このようなケースについても、同様に処罰の対象とする必要がある。また、従業員による不正に対しては刑罰の適用だけではなく、業者自体が服務規定により処分を行うことも必要である。
- (4) 例えば、信用情報機関の内部の者、あるいはネットワークに侵入した外部の者が登録データを改ざんする等情報の偽造を行った場合、電磁的記録不正作出罪等刑法による一定の措置はあるが、個人信用情報の内容の正確性が担保されることは、信用情報システムの維持に不可欠であること、また、情報主体にとっても情報の内容は個人の信用を左右するものであることから、同法が適用できない範囲に対する措置も必要である。

- (5) 業務受託者による不正行為として、情報を不正に蓄積し、それを利用・提供することもあり、こういった行為に対する措置も必要である。
- (6) 外部のものによる不正行為として、窃取、詐欺、強迫その他不正の手段により情報を取得することがある。従来、情報が記録されたフロッピーディスク等の「物」を窃取した場合には窃盗罪の適用が可能であったものの、情報自体の窃取は処罰できなかったが、個人情報情報の不正な取得を刑罰の対象とする必要がある。
- (7) 近年の情報漏洩事件の多発は個人情報情報が名簿業者等で売買され、流通されるようになったことが一つの要因として考えられる。情報の不正な流通を防止することは、これらの事件の再発の防止にも役立つものと考えられる。この観点から、不正取得又は不正提供された情報であると知りつつ情報を入手し、その利用・提供を行うことに対する措置も必要である。

11. 自主規制による対応

- (1) 与信業者等が個人情報情報の保護に関して十分な対応をとらない場合には、当該業界が信頼を失うだけでなく、与信システム全体に対する悪影響も懸念される。また、繰り返し述べているように、個人情報情報の保護利用のためのルールは、法的措置のほかに自主ルール等において重層的に手当することが望ましい。こうした観点から、与信業者等は、この懇談会において検討された具体的な措置を実現するため、できるだけ早期に自主ルールの一層の整備を図り、そのルールに則った対応を行っていくことが求められる。
- (2) 法的措置の対象とする情報の範囲については、ここでは一定の個人情報に限って検討を進めてきたが、自主ルールの対象としては各業界が収集・保有・利用する個人情報全般とすることが望ましい。
- (3) 自主ルールの整備に当たっては、ここで検討された措置のみならず、個人の自己情報コントロール権の保護に資するための措置をさらに詳細に検討する必要がある。中でも、情報主体から情報収集するに当たっての同意文言や説明方法、苦情処理手続きを明確化すること、情報主体の権利や信用情報機関の情報登録・照会のシステムを分かりやすく説明すること等は、早急に検討・実施されるべき課題である。また、無差別的なダイレクトメールを抑止することなども自主ルールの重要な要素である。
- (4) 業界ごとに明確な自主ルールとしてガイドラインをまとめる際には、実効性の確保が重要である。ガイドライン違反への制裁が直接的な方法であるが、ガイドラインを遵守する企業に対してマークを付与するというのも一つの方法として考えられる。マーク付与制度が有効に機能するためにはマークに対する一般消費

者の認知が不可欠であることを踏まえ、このような制度の導入に当たっては、制度の周知を進めるとともに、ガイドラインを遵守していないにもかかわらずマークを掲げる事業者への対応策についても検討する必要がある。

- (5) 本来、企業ごとに規模も業務内容も異なることから、個人情報保護のために必要となる措置の在り方も個別企業ごと異なるものであるが、法律は守るべき最低限の基準を示しているにすぎない。また、業界ごとのガイドラインにも個別企業の状況を完全に反映させることはできない。そこで、企業ごとに異なる自主規制に法的な意味づけを与え、法的に自主規制の遵守を担保する手法（enforced self-regulation）も検討に値するものと考えられる。具体的には、各企業にそれぞれ策定されている自主規制を監督官庁が承認し、かつ各企業内にその遵守をモニターする監査部門の設置を求め、自主規制への違反に対して企業内モニター部門の指導が効果を発揮しない場合には、営業停止等の行政処分等をするなどといった方法の検討が考えられる。

12. 情報システムの整備による対応、情報保護に関する標準化への動き

- (1) 個人情報情報の保護には、制度的な面での整備を進めるとともに、技術的な対応も不可欠である。特に、近時、情報関連技術は急速に進んできており、自己に関する情報をコントロールしやすい情報システムづくりに向け、これらの成果を取り込むことが重要である。
- (2) システム作りに当っては、様々の対応が考えられるが、例えば、データベースにアクセスするためのパスワードや暗号化されたキーを、債務者と与信業者がそれぞれ保有し、債務者の情報を名寄せするには両方のキーが必要となるシステムも考えられるのではないかと意見もあった。
- (3) 情報保護に関する標準化については、1996年5月、ISO（International Organization for Standardization：国際標準化機構）に個人データ及びプライバシー保護に関する諮問委員会が設置され、国際的に検討が始まったところであり、これらの情報システムの整備に当たっては、その動向を踏まえるとともに、我が国での情報保護に向けた対応をISOでの検討にも反映させていくべきである。

13. 地方公共団体の役割

- (1) 平成9年4月現在、1,312の地方公共団体において、個人情報に関する条例が制定されており、制定団体数の割合は全団体数の39.5%となっている。また、条例制定団体のほかに、規則等により個人情報保護対策を講じている団体が、都道府県及び市町村で804団体あり、合計すると2,116団体（全団体