

韓国における個人情報の保護(1)

李 仁 那

永 山 茂 樹

目 次

はじめに

I. 個人情報保護に関する基本的理解

1. プライバシー権
2. 私生活の自由と知る権利の衝突
3. 個人情報の概念
4. 個人情報侵害類型と個人情報保護のための接近方法
5. 小括

II. 個人情報保護法の概容

1. 公共機関の個人情報保護に関する法律（個人情報法）
2. 民間部門の個人情報法制（情報通信網利用促進等に関する法律）
3. 個人情報保護マーク制度
4. 韓国における個人情報保護法の課題
5. 小括

はじめに

本稿は、韓国において個人情報の保護がどう考えられ、保護策がどう講じられ、またどのような課題が論じられているか、電子住民カードや教育行政情報システムなどの具体的事例を交えつつ紹介するものである。

この作業は、日本における個人情報保護のあり方を検討するためにも有意義であろう。なぜなら第一に韓日両社会とも経済のボーダーレス化に加速されながら情報のハードとソフトの整備を推進しており、そこで個人情報をいかに侵害から保護するかという課題を共有する。第二にこの課題を、

平成16年4月3日受理

伝統的な個人主義観念が十分に発展・定着していない非西欧社会でどう解いていくのかという点においても、両社会は同じ地平に立っている。第三に情報化と並行して国家権力の民主化に意識的に取り組む韓国の状況を通じ、現代国家における個人情報の保護と権力の民主的統制の関係を考える手がかりを得られるからである。

I. 個人情報保護に関する基本的理解

1. プライバシー権

個人情報を目指す場合に、秘密やプライバシーという言葉がよく使われる。秘密は他人に知られないことで自分に利益がある事実であり、それが保護される権利がプライバシー権の一部分である。

個人情報とはプライバシーと同じ意味で使われているが、厳格に言えばプライバシーは個人情報という概念だけで覆いきれるものではない。ある個人の個人情報に対する不適切な接近、収集、分析、保存はその個人に対する他人の認識と行動に影響を与えるし、その個人の社会的地位、評価、財産、安全などにも悪影響を与える。したがって、個人情報は客体的存在としての保護対象である。一方、プライバシーの保護対象は個人情報自体であるというより個人情報に関する権利であるといえる。つまり、プライバシーは個人情報に関して情報主体がその権利を行使し、守ろうとする側面を強調したものである。韓国における個人情報の問題を論ずるにあたり、まずこのプライバシー権概念の検討から着手しよう。

プライバシー権とは19世紀末にアメリカにおいて生成された概念であり、1890年にウォーレン(S.D.Warren)とブランドイス(L.D.Brandies)の論文“The Right to Privacy”で初めて登場したとされる。ブランドイスはプライバシー権を「ひとりで放っておいてもらう権利」(the right to be let alone)と定義し、民主主義における最も重要な自由として憲法に反映すべきであるとの主張をした。この論文の発表以来独立した権利として認められ始め、アメリカの判例法上も認められるようになった。その根拠は幸福追求権であるとされる⁽¹⁾。このように消極的な権利として定義される古典的プライバシーは20世紀半ば以来、拡張的に修正され、現在では積極的な権利として定義される個人情報の自己コントロール権をあわせもつ概念と理解されている。この個人情報の自己コントロール権はコンピューターや情報通信技術の発達により個人情報が大量に処理、利用される情報化社会において定立された権利である。

情報化社会においてプライバシー権は大きく五つの意味を持つ。第一に「ひとりで放っておいてもらう権利」を意味する。これは古典的考え方の延長線であるが、個人の身体や物理的接近からの自由だけを意味するものではない。電子メール、ショートメッセージサービス(SMS)などのような仮想的接近ヴァーチャルなも含まれる。いわばオンオフラインからの他人の接近を拒否する権利を持つ。第二に自分に関する情報が、自分が望んでいない方

式で利用されない権利を意味する。これは本人の同意なしに個人情報が売買、露出されない権利を意味する。第三に自分も知らないうちに自分に関する情報が他人によって収集されない権利を意味する。CCカメラによるモニタリング、クッキー・ログファイルによる記録もこれに該当する。これは政府や企業が個人情報を収集する時告知義務を負うことを意味する。第四に自分が正確にまた正しく表現される権利を意味する。データベースに入っている個人情報はその人自体を表すので、個人の虚像を作らないためにも個人情報の無欠を維持することは重要なのである。ここから派生する権利が自己情報に対する接近と決定である。情報主体がデータベースに入っている自己情報を閲覧し、修正することで個人情報のエラーが防止できる。第五に自己情報が持つ価値に対して補償される権利を意味する。情報化社会において多くの場合個人情報は財産的あるいは商品的価値を持つ。個人情報が収集・活用される時、情報主体にどのような形態であれ適切な補償をしなければならない⁽²⁾。

プライバシーという用語は韓国で私生活と翻訳される。1980年制定の旧憲法第16条は「すべての国民は、私生活の秘密及び自由を侵害されない」と、また1987年制定の現憲法は第17条で「全ての国民は私生活の秘密と自由を侵害されない」と、プライバシー権(広義の概念では住居の不可侵、通信の秘密等をも含む)を規定している。このように韓国憲法はプライバシー権を人格権の一部門として認めながら、個人の一般的人格権(第10条の定める幸福追求権)とは別の自由権で独立して規定するという特殊な構成を取る。要するに、憲法第17条の私生活の秘密と自由⁽³⁾≒プライバシー権⁽³⁾≒人格権という図式が成立する。

憲法第17条の「私生活の秘密と自由の保障」は、私生活の秘密の不可侵、私生活の自由の不可侵及び自己情報コントロール権をその内容とする複合的性格の権利である。私生活の秘密の不可侵は個人が内緒にしようとする私的事項や名誉、信用、そして名前、肖像、経歴、イメージなど、個人の人格的領域の不可侵を意味する。私生活の自由の不可侵は、私生活の自由な形成と展開そして私生活を邪魔されない権利を意味する。自己情報

コントロール権は、狭義には自己情報の閲覧・訂正・使用中止・削除等をその内容とするが、広義には自己情報を自律的に決定・管理する権利である。私生活の秘密が公権力あるいは他人に対するより消極的・防衛的性格のものならば、私生活の自由と自己情報コントロール権は請求権的性格を持つより積極的・能動的性格のものであり、知る権利としての性格も兼ね備える。90年代韓国におけるプライバシー理解の進展過程の中でそれを確認したい。

まず憲法裁判所は刑事確定訴訟記録コピーを拒否した被請求人（ソウル地方検察庁検事）の行為に対して、被請求人は請求人が要求したコピーの具体的内容を確認・検討した上で、その内容の公開が関係人の基本権を侵害する素地があるかあるいは国家安全保障・秩序維持・公共の福利を侵害する恐れがない場合、その内容の閲覧・コピーを許容する措置をとることは憲法第10条が明示する国家の基本権保障義務を誠実に遂行することであるとされた。そして、現行実定法に請求人の刑事確定訴訟記録を閲覧・コピーする権利の明文規定がないとの理由でコピーを拒否した行為は、憲法第21条により保障される知る権利を侵害し、違憲であると決定した（憲裁決1991. 5. 13, 90憲マ133⁶⁾）。

ところで個人情報法に関する立法は大別して2つの形態に分類される。一つは個人情報保護範囲を拡大して民間保有情報、政府保有情報、電算以外の情報までもその規制対象にする場合であり、もう一つは政府の保有する電算処理の情報だけを規制対象にする場合である。後者が日本の場合（1988年行政機関の個人情報保護法）であり、韓国はそれをモデルにしたと言われている。すなわち1994年、公共機関の個人情報保護に関する法律（以下個人情報法。その詳細はⅡで論じる）を制定・公布し、自己情報コントロール権を保障した（もっとも日本では韓国とは違い、国の立法措置に先行的に各地方自治体は条例で個人情報を保護し、行政機関の個人情報保護法を補完していた⁶⁾）。同法にいう自己情報コントロール権は具体的に自己情報閲覧請求権（個人情報法第12条、第13条）、自己情報訂正請求権（同法第14条）、自己情報使用中止・削除請求権をその内容とする。その内、個人情報閲覧請求権は知る権利としての性格をも

ち、情報公開請求権が保障される場合もある。

憲法レベルの議論に戻ろう。大法院(1998. 7. 24, 96ダ42789)は憲法第17条による私生活の秘密と自由の保護範囲を判示している。この事例は、国軍保安司令部が約1,300人の民間人を視察し（情報収集、尾行、スパイ、探聞等）、個人身の上資料綴じ、電算個人カード及び索引カード等を保管・管理してきた事実の内部暴露を契機に、カンドンキョ外144人が大韓民国を相手にし提起した損害賠償訴訟である⁷⁾。法廷はその文書の提出を命令したが被告は応じなかったので、法廷は命令に応じなかった事情を総合判断して原告主張（個人情報収集・管理事実）を真実として認めた。判決で「憲法第10条は“全ての国民は人間として尊厳と価値を持ち、幸福を追求する権利を持つ。国家は個人が持つ不可侵の基本的な人権を確認してこれを保障する義務を負う”と規定する。また、憲法第17条は“すべての国民は私生活の秘密と自由を侵害されない”と規定してこれらの憲法規定は個人の私生活活動が他人から侵害されるか私生活がむやみに公開されない消極的な権利は勿論、高度に情報化された現代社会で自分に対する情報を自律的に統制することができる積極的な権利までも保障しようとするところにその主旨がある」と解釈し、「被告人傘下国軍司令部が軍と関連したスパイ収集、特定軍事法廷管轄犯罪捜査等法令に定められた職務範囲を超えて民間人である原告を対象にし、日ごろの動向を監視・把握する目的で持続的に個人の集会・結社に関する活動や私生活に関する情報を尾行、スパイ活用、探聞採集等の方法で秘密に収集・管理したとすると、これは憲法が保障する原告の基本権を侵害するもので不法行為が構成される」とした。また原告中には公的人物である盧武鉉（現大統領）、文東煥（元国会議員、現牧師）等もおり、国民の知る権利の対象として私生活の秘密と自由が一定の範囲内で制限される場合もあるが、それは公共の利益になるという点でその根拠があるものであり、一般国民の知る権利と無関係に国家機関が日ごろの動向を監視する目的で個人情報を秘密に収集した場合は、その対象者が公的人物である理由だけでは免責されないとした。

紹介した決定・判決は憲法10条あるいは第17条

の規定が自己情報コントロール権を保障するとしたが、これを巡って学説は分かれている。

第1説は、憲法第17条を自己情報コントロール権の直接的根拠とみなす(多数説)。この説は、同条項が情報化社会での個人情報侵害の深刻性を考慮して新しく創設されたものであって、特に1987年憲法が第127条第1項⁽⁸⁾で情報の開発を国家の任務と規定したこともあって、憲法制定者の意図が個人情報保護の必要性にあったと見なければならぬと主張する。そして自己情報コントロール権を核心要素とする私生活の秘密と自由は、プライバシー権の一人権である同時に、第10条前段「すべての国民は人間としての尊厳と価値を持ち、幸福を追求する権利を持つ」と定めた人間の尊厳性規定、第37条第1項「国民の自由と権利は憲法に列挙されないという理由で軽視されない」と定めた列挙されていない権利保護条項とともに、人格権の根拠規定であると解している。この説の特色は、自己情報コントロール権が人間の尊厳を確保するのに必要不可欠な私生活保護の次元で認められるということを特に強調している点にある。

第2説は、第17条の内容を広く解釈する場合、その他基本権条項を全部包括する基本権になるから、第17条を「私生活をみだりに公開されない自由」と狭義に把握し、消極的プライバシーの根拠規定としてみなす考え方である。金チョルス教授は「われわれの憲法は私生活の秘密と自由を自由権条項で規定しているのだから、私生活の秘密と自由を消極的権利としてみるのが妥当である。しかし、私生活の秘密・自由を自由権としてみるとしても、自己の情報をコントロールする権利を否定するわけではない。しかし、この情報に対する自己決定権は第17条ではなく、憲法第10条で保障されているとするのが妥当である」として⁽¹¹⁾いる。

第3説は、自己情報コントロール権は第17条で直接的に保護されるとしながらも、第10条の人間の尊厳と価値、幸福追求権規定と憲法前文、第4条⁽¹²⁾と第8条⁽¹³⁾の自由民主主義的基本秩序規定がこれを補完するとする考え方である。⁽¹⁴⁾⁽¹⁵⁾

これら各説はその根拠に違いはあるけれども、プライバシー権・自己情報コントロール権のいずれも憲法上の権利と捉える点では共通するように

思われる。

しかし第1説は自己情報コントロール権を私生活の保護という狭い領域に巻き込んでいるという点で、第2説はその根拠を人間の尊厳と幸福追求権に求めることによる個人自立権の伸張という側面に固定させるという点で、批判がある。第3説は自己情報コントロール権を個人の私的人格の保障にとどまらず国家の意思決定と密接な意味を持つ人格の公的性格を看破している点で一歩進んだ主張ではあるが、自由な人格の保障が自由民主的意思決定の正当性を担保するために、自由な人格の前提で認めるという点を強調するのにとどまることによって、この権利が権力行使の民主性を担保するのに重要な権力統制的政治的権利としての性格を持つという点を看過している。⁽¹⁶⁾金鐘鐵教授のこの批判は、自己情報コントロール権の保障が、たんに私人の権利を保障するにとどまらず、権力の民主的統制と密接につながることを指摘した点で、注目される。

なお日本国憲法は、韓国憲法第10条の「幸福追求権」に該当する規定をもちながら、他方で同第17条の「プライバシー権」に該当する規定を欠く。そのため、プライバシー権のみならず自己情報コントロール権の根拠についても、必然的に憲法第13条の「幸福追求権」規定に依拠せざるを得ないという事情を抱えている。したがって両国の議論をただちに並べて比較することには慎重さが必要だろう。

2. 私生活の自由と知る権利の衝突

すべての国民は自分の領域を持つ自主的人格の主体である同時に、社会共同体の構成員として他人と社会生活を形成していく社会的人格の主体である。それゆえ、自分の領域を主張することに一定の限界がある。私生活の秘密・自由も絶対的権利ではなく、国家安全保障、秩序維持、公共福利のため必要な場合法律により制限される。それは知る権利においても同様である。知る権利とは一般的に、接近できる情報源から意思形成に必要な情報を収集し、収集した情報を取捨選択する自由を言う。個人にとっては公共機関と社会集団等に対して情報公開を要求する権利を意味し、言論機関にとっては公共機関と社会集団等に対して情

報公開を請求する権利だけでなくそれに対する取材の自由をも意味する（大法院1999. 9. 21、97ヌ5114）。韓国では1996年に公共機関の情報公開に関する法律が制定され、知る権利が保護されている。このような情報の受領・収集源に対する妨害排除、情報閲覧請求権をその内容とする知る権利は、社会の情報化に伴って私生活の秘密・自由と衝突を頻繁に起こしている。私生活の秘密と衝突する場合、どのように調和させるかという判断および判断の基準論が重要となるが、それにはいくつかの説がある。

第一に権利放棄理論である。一定の事情下で私生活の秘密と自由を放棄したとみなされる場合、それに対する権利が消滅するから私生活が公開されても侵害行為にならないという理論である。第二に公益の理論がある。国民の知る権利の対象となる事項は国民に知られることで公共の利益になるという理論である。したがって、公正な解説、犯罪人の逮捕、公衆保健と安全、犯罪被害者公開等は私生活の秘密と自由の侵害にならない。第三に公的人物理論がある。私生活の秘密と自由が侵害されたと主張する者の社会的地位によって、私生活の秘密と自由の限界が決定されるべきであるとする理論である。⁽¹⁹⁾

判例において、まず大法院は「人格権として個人の名誉の保護と表現の自由の保障という二つの法益が衝突した時、その調整をどのようにすべきかは、具体的な場合に社会的なさまざまな利益を比べて表現の自由から得られる利益・価値と人格権の保護によって達成される価値を比較衡量してその規制の幅と方法を定めなければならない」とした（大法院1988. 10. 11. 85ダカ29）。憲法裁判所は「言論媒体の名誉毀損的表現に実定法を解釈適用する時には、言論の自由と名誉保護という相反する憲法上二つの権利の調整過程に次のような事情を考慮しなければならない。すなわち、当該表現による被害者が公的人物であるかそれとも私人であるか、その表現が公的な関心事案に関するものであるか単に私的領域に属する事案であるか、被害者が当該名誉毀損的表現の危険を招来したか、その表現が客観的に国民が知るべき公共性・社会性を取り揃えた事実（知る権利）として世論形成や公開討論に寄与するかなどを総合して、

具体的な表現内容と方式によって相反する二つの権利を有形的に比較衡量した比例関係を計算して言論の自由に対する限界設定をする必要がある」とした（憲裁決1999. 6. 24、97憲マ265）。

上述した諸説は批判の余地がある。すなわち、権利放棄理論は本人の意思を無視しており、公益理論は名誉毀損との区分が困難であり、公的人物理論は公的人物の私生活の秘密と自由の保障を看過している。私見でも、私生活の秘密・自由と知る権利間の調整はこれらの理論を総合し、具体的事案により判断することが妥当である。大法廷と憲法裁判所の判断で採られた両法益の具体的事案による比較衡量の方法を支持したい。

3. 個人情報の概念

ではプライバシーとして保護され自己情報コントロール権の対象となる個人情報とはどういった情報を指すのか。個人情報侵害問題の深刻性を認知するため、またその解決策を探るために個人情報の明確な定義が必要である。

まず公共部門におけるそれは、1994年の個人情報法が定義する。同法第2条第2項は「生存する個人に関する情報として当該情報に含まれている姓名・住民登録番号などの事項により個人を識別できる情報（当該情報だけでは特定個人が識別できないとしても他の情報と容易に結合して識別できるものを含む）」と定義している。しかし同法第1条で「公共機関のコンピューターによって処理される個人情報の保護のためにその取り扱いに関して必要な事項を決めることで公共業務の適正な遂行をはかることと同時に国民の権利と利益を保護することを目的にする」とあるように、公共機関の扱う個人情報でコンピューターによって処理されるものだけを対象にしている限界も指摘される。

民間部門を統制する代表的法律である情報通信網利用促進及び情報保護等に関する法律第2条は「個人情報とは生存する個人に関する情報であり、当該情報に含まれている姓名、住民登録番号等の事項によって当該情報を識別できる符号、文字、声、音及び映像等の情報（当該情報だけでは特定個人が識別できないとしても他の情報と容易に結合して識別できるもの）をいう」と個人情報を定

義している。これは多様な個人情報認識手段が個人情報に含まれることとそれら情報のプライバシー概念を明らかにしている。そこで、個人情報の範囲は固定されることなく持続的に拡大していくと解される。情報化社会の発展はクレジットカード暗証番号、電子メールアドレス、クッキー情報、DNA情報など新しい個人情報を際限なく作り上げていくからである。また個人情報は個人が保有する情報だけでなく、信用情報、取引情報、内面の秘密、心身の状態、社会経歴、経済関係、生活・家庭・身分関係で分類される各種情報がその対象になる。個人情報の主体は自然人であり、法人あるいは死者、失踪宣告等関係法令により死亡したと扱われる者は個人情報の主体にはなれない。

個人情報の内容は基本データ、^{センシティブ} 敏感な情報、非常に敏感な情報、無意識的提供情報とで分けられ、具体的項目は次のとおりである。基本データは、個人属性情報であって、住所、姓名、家族、配偶者、就学、就職先等である。敏感な情報は、あまり他人に知られたくない情報であり、個人信用情報（金融、資産関連）、趣味、身体特徴、学歴、結婚経歴、性格判断・心理テストの結果等である。非常に敏感な情報とは、特に他人に知られたくない情報であり、病院での診療記録、看護・検査記録、診療費請求明細書、人種、民族、宗教、思想、信条、政治的見解、労働組合の加入有無、保健医療及び性生活等である。無意識的提供情報は意識的に提供したものではないがマーケティングなどで活用されるものであり、商品等の購入時期、商品名、金額、支払方法などがある。

4. 個人情報侵害類型と個人情報保護のための接近方法

個人情報は古典的プライバシー権や個人の秘密のように完全な隠秘の対象ではないが、一定の統制下で、情報主体の自己決定権の活用対象となる個人情報である。そしてその侵害類型は侵害行為による分類方法により、個人情報の収集、個人情報の目的以外の二次的利用、個人情報のエラー（error）、不当なアクセス（improper access）に分けられる。以下インターネット法律の論壇と情報通信部発刊『個人情報保護白書』に依拠してまとめよう。⁽²¹⁾

第一に個人情報の収集である。合法的で正当な手続による個人情報の収集は何の問題にもならない。例えば、情報サービス業者からあるサービスを受ける目的で、情報主体者である個人が自己情報を提供することは、正当な手続による場合である。では不適切な個人情報の収集であるが、たとえばネットワーク管理者の許可を得ずに公共機関あるいは企業などのコンピューターに侵入して個人情報を収集する行為、インターネットで繋がっている個人コンピューターに侵入して個人情報を収集する行為などが、これに該当する。また情報主体の同意ない収集、個人情報収集の際告知・明示義務を怠った行為、情報主体の同意撤回・閲覧あるいは訂正要求に応じないかこれを収集より簡単にできる措置をとらない行為などが含まれる。個人情報法は犯罪捜査や裁判に必要な場合、法律が規定した業務遂行のための場合、当事者の同意がある場合等を除き、個人情報を外部に提供することや他の目的に利用することができないように制限している（第10条）。また警察庁保安業務規定は、身元調べ対象者を公務員任用予定者、秘密取り扱い認可予定者、海外旅行者、国家重要施設の装備及び資材を管理する者など国家保安上必要だと認められる場合に制限している。しかしこの制限にもかかわらず、今もなお個人情報の秘密収集は公然と行われている。個人情報が公然たる秘密として部分的に収集されることも個人情報収集による侵害例である。個人の一部情報を収集し、リストを作成する行為は個人に対する虚像を作り出す。企業による新入社員の身元調査、労働組合での活動経歴などの特定情報に基づいて作られたブラックリスト等がその例である。

第二に個人情報の収集目的以外の二次的使用である。特定の目的で収集された個人情報が情報主体の同意なしに他企業に取引され、再利用される場合がこれに当たる。また、コンピューター、情報通信技術の発達には各々持っている企業の個人情報を容易に統合・交換させ、二・三次の個人情報を生み出し、それが悪用される場合もある。デパートの持つ情報が流出し犯行対象選定に利用された事例や、医療保険関連情報が選挙に利用された事例などがその例である。

第三に個人情報のエラーである。個人情報は静

的情報 (static private information) と動的情報 (dynamic personal information) で分けられる。そのうち、動的情報は時間が経つにつれて変わるものであるが、変わった内容をデータベースに反映しなかった場合、個人の虚像が作られるおそれがある。エラーのあるデータベースは企業にとってデータベースマーケティングに非効率的の影響を与えるだけでなく、情報主体である個人にはプライバシー侵害問題が生じる。実際、住民登録番号の誤った入力により犯罪者と誤解され、警察に不当な取り調べを受けた事例もある。

第四に不当なアクセスである。ハッカー (hacker) など不当なアクセスは個人情報の流出、変更、破壊につながる。データベースから特定個人に関する情報を不当に取得し、悪意で変更、外部に流出させた事例や国民年金保険職員が加入者情報を民間企業に渡した事例がある。

これらの侵害類型に対して、個人情報を保護するためには大別して4つの接近方法があると言われる。第一に立法的規制方法である。政府が直接介入して、民事・刑事的な処罰により保護する方法である。国家は社会構成員全体の利益を守る義務があり、特定の社会的行動は制限することができるという発想に基づいており、ヨーロッパでとられる個人情報保護の手法でもある。アメリカは知識情報社会の発展に比重を置くが、伝統的にヨーロッパの国々は個人情報侵害のような情報化の逆機能を防止することにもっと大きい比重を置く。

第二に財産権的規制方法である。個人情報に対する財産権を個人に付与する方法である。財産権の付与により、個人情報を個人の同意なしに第三者に販売することは不法行為になる。また、承諾があった場合でも販売代金の持分に該当する権利は個人に帰属される。この方法は、プライバシー侵害に対する適切な補償請求権を可能にし、適切な水準の個人情報の流通を維持させるとの見解である。しかしこの方法は實際上、いくつかの問題点がある。財産権の行使のため、自分の情報がどこへ流出し流通しているのかのモニタリングが必要である。だがそれは決して容易ではなく相当な費用もかかり、財産権行使から得られる利益より多額の費用がかかってしまい、財産権の行使を諦めたほうが利益かもしれないからである。また個

人情報という財産は家族関係、社会関係などで共同財産権に対する一部の持分としての形態が多いが、共同財産権の行使は容易ではなく、その持分も大きくないはずであるからその行使には限界がある。

第三に自由放任的市場機能による方法である。言葉どおり、市場機能に任せておく方法である。個人のプライバシーを侵害した企業のイメージが悪くなれば、結局個人情報保護の消極的な企業は、市場から退出させられるという前提に基づく。しかし例えば中古自動車の場合、買う側は売る側より自動車について多くの情報を持つであろう。そうすると中古車を高く売ろうとする販売側より情報の少ない消費者は、品質に比べて割高で買う確率が高くなる。その結果、消費者は中古車を信頼しなくなる。問題のないいい中古車はいい値段を得られないので市場に出なくなり、問題のある中古車だけが市場に出るようになる。それが市場崩壊に繋がるのである。この方法は市場の失敗につながらないように企業が個人情報政策を実際に遵守しているかモニタリングが必要だが、情報の非対称性⁽²³⁾の下では費用も時間もかかる。

第四に自律規制方法である。アメリカを中心として進められている方法であり、企業あるいは業界自ら個人情報保護措置をとるよう誘導するものである。自律規制が自由放任と異なる点は企業自ら個人に個人情報侵害問題を簡単に効果的な方法により解決することを保障する点にある。つまり、市場の失敗原因を除去して、個人情報保護措置をとらない企業は市場から退出されるようにすることで企業自ら費用と努力をかけて個人情報措置をとるよう誘導するという点にその差がある。企業は不満を調査する手段を提供し、個人がどのような方法でシステムへ接近できるかを知らせなくてはならない。企業等は相当の費用や努力を払わなければならないが、企業イメージ向上による便益を勘案すると相対的にその費用は少ないと考えられる⁽²⁴⁾。

5. 小括

個人情報保護のための諸方法を4で述べた。どの方法がよいか結論を急ぐ前に、人々が自己情報に対する認識を深めることの重要性を強調したい。

公共機関や企業に何気なく提供した自己情報がどう使われているのか、情報化社会において個人情報にどの程度の価値をもつかを認識できれば、情報の悪用・誤用はある程度事前に予防できる。また自己情報の価値に対する十分な認識は、諸説が強調する自己情報コントロール権行使の定着にも寄与するであろう。これは韓日両社会に共通する課題でもある。

そのうえで、法はどういった基本スタンスをとるべきであろうか。韓国は個人情報保護に関して、公共部門と民間部門を区分して適用する法体系を取る。だが政府が民間部門をいちいち監視し規律することは、民主的市場論理にも合わず無理な点が多いのではないか。なぜなら政府による法的規制方式は、急速に変化する情報化社会に迅速に対応できず、いきつくところ頻繁な法改正問題をもたらすはずである。また無国境的環境下で移転する個人情報に対応して、各国の個人情報保護関連規制を調整することの困難さが、立法のコストを増加させるであろう。したがって民間部門においては法的規制方法ではなく、自律規制による個人情報保護を原則とすべきではないかと思われる。

もっともこれでは強制的手段を欠き、個人情報の保護水準は法的規制をとった場合と比べて劣る危険がある。自律規制成功の鍵は、前述したように自己情報に対する価値の認識、あるいは人々の権利意識の高揚である。自己情報に対する価値の無知は、企業をして市場から退出させないからである。

一方、公共部門に関しては立法的規制の強化が妥当ではないだろうか。それは公共部門における個人情報は財産、金融、信用、医療関係の信頼性のあるとされる敏感な情報が多く、その情報の流出は個人に精神的、財産的、社会的に莫大な被害をもたらすからである。また公共機関の有する情報を政府が管理することは、ことの性質上、民間部門の場合より容易であり、また政府の必要性により収集される個人情報を政府が管理することは当然でもあるからである。したがって、法的規制による関連公務員の処罰規定の強化、個人情報保護措置の強化などが望ましいと考えられる。

II. 個人情報保護法の概容

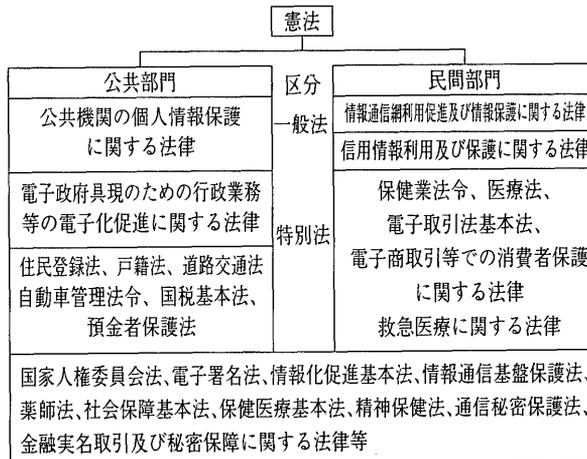
前述したように韓国の個人情報保護は、公共部門と民間部門を総括する一般法を設けるかわりに、公共部門と民間部門を区分して規律する法体系をとる。公共部門分は行政自治部の「公共機関の個人情報保護に関する法律」が、民間部門は情報通信部の「情報通信網利用促進と情報保護に関する法律」が主に規律するが、そのほか「通信秘密保護法」「信用情報の利用及び保護に関する法律」「金融実名取引及び秘密保護に関する法律」「電気通信事業法」等があり、各部分別に個人情報保護規定が散在する（図1参照）。もちろん、サイバー空間での人権侵害行為が刑法上の個別犯罪構成要件を満たす場合は刑法で規律される⁽²⁵⁾。また民間部門では、強制規範以外にも業界が自発的に個人情報を保護するよう支援する個人情報マーク制度（後述）が導入されている（図2参照）。

〈図1〉韓国の個人情報関連法令

立法年度	立法名称
1983年	電気通信基本法、電気通信事業法
1986年	電算網普及拡張と利用促進に関する法律（99、2000改正）
1989年	電波法改正（61年制定）
1991年	貿易業務自動化に関する法律
1993年	通信秘密保護法、金融実名取引及び秘密保障に関する緊急財政経済命令
1994年	公共機関の個人情報保護に関する法律、情報通信設備に関する安全信頼性基準、工業及びエネルギー基盤造成に関する法律
1995年	コンピューター犯罪対応規定に関する刑法改正
1997年	金融実名取引及び秘密保障に関する法律、公共機関の情報公開法
1999年	情報通信網利用促進等に関する法律（制定）
2000年	情報通信網利用促進及び情報保護等に関する法律（制定） 情報通信網基盤造成法（制定）

出典：鄭英和『電子商取引法』多山出版社、320頁より

〈図2〉韓国の個人情報関連法律体系



出典：崔月和『電子政府とプライバシー保護』討論文29頁より

1. 公共機関の個人情報保護に関する法律（個人情報法）

公共部門における個人情報保護法の要請に関しては行政電算網の構築と密接な関係がある。1983年政府は行政、金融、教育研究、公安等において、国家機関電算網事業を進め始めたが、それが個人情報保護の強化の必要性を台頭させた。政府により進められてきた電算網事業と電算化作業は公共機関でのコンピューターによる個人情報の処理作業を拡大させる一方、地域間、機関間の情報流通体制を確立させた。このような行政部門の電算化は⁽²⁶⁾民願処理期間の短縮、居住地中心の民願処理から全国的な民願処理へとその便宜性が向上され、効率的な行政運用が可能となり、情報処理の幅と深さが大幅に拡張された。

しかしこのような便宜性と裏腹に、個人情報の不当使用、無断流出、乱用等による個人の私生活の侵害が問題となり始めた。当時、個別法令（住民登録法、国家公務員法等）の宣言的処罰を中心とした法令体系はこのような逆機能を効率的に予防し、対処することに限界があった。このような実情に対し、1989年2月国際人権擁護連盟韓国連盟の法制定申立てを皮切りに言論機関、関連団体からの要請が相次いで起き、政府は1994. 1. 17法律第4734号「公共機関の個人情報保護に関する法律」（個人情報法）を制定した。その後1999年には、個人情報利用及び提供要件の強化、本人閲覧制限事由緩和等を内容とする改正⁽²⁷⁾があった。

(1) 主要構成内容（本文5章25条、附則）

第1章 総 則

目的、定義、適用範囲、他の法律との関係

第2章 個人情報の収集及び処理

個人情報の収集、個人情報ファイルの保有、事前通報、個人情報ファイルの広告、個人情報ファイル台帳作成、個人情報の安全性確保、処理情報の利用及び提供の制限、個人情報取扱人の義務

第3章 処理情報の閲覧及び訂正

処理情報の閲覧、処理情報の閲覧制限、処理情報の制限、不服請求、代理請求

第4章 補 則

手数料等、資料提出の要求等、意見提示及び勧告、個人情報審議委員会、政府投資機関等の指

導・監督、公共機関以外の個人あるいは団体の個人情報保護

第5章 罰 則

罰則、両罰規定、罰則適用に関しての公務員擬制
(2) 目的及び適用範囲

この法律は公共機関のコンピューターによって処理される個人情報の保護のため、その取扱に関して必要な事項を決めることで公共業務の適正な遂行をはかるとともに国民の権利と利益を保護することを目的とする（第1条）。この法律の適用対象は公共機関である。第2条2項によれば、ここで公共機関とは国家行政機関、地方自治団体その他公共団体中大統領令が定める機関をいう。この法律の保護対象は公共機関の保有する個人情報であり、個人情報とは生存する個人に関する情報として、当該情報に含まれている姓名、住民登録番号などの事項によって当該個人を識別することのできる情報をいう（第2条）。但し、法人あるいは団体の情報、死者に関する情報（遺族との関係で一定期間保護対象になれると解される）、他の法律に特別な規定がある場合、統計法により収集される個人情報と国家安全保障と関連して情報分析を目的で収集あるいは提供要請される個人情報の場合はこの法律の適用対象から除かれる（第3条）。現在、個人情報に関して特別な規定を設けている他の法律として金融実名制法、公職者倫理法、医療保険法、住民登録法などがあり、これらの法との衝突を防ぐために第3条の規定が設けられていると考えられる。

(3) 個人情報収集・管理

公共機関による個人情報収集は、最小限の範囲内での収集を原則とする。まず第4条において、公共機関の長は思想・信条等個人の基本的人権を著しく侵害する恐れのある個人情報を収集してはならないと規定している。このような規定を設けた理由は、個人の基本的人権を侵害する恐れのある情報は収集段階から制限するという予防的処方のためである。しかし、このような個人情報の収集も情報主体の同意があるか、他の法律に収集対象として明示されている場合は可能である（第4条）。

第5条は公共機関の個人情報保有範囲を必要

な範囲内と限定している。個人情報保有の必要性判断は一次的に公共機関の長が決定し、二次的にはファイル保有の事前通報を受けた行政自治部長官、関係中央行政機関長等の監督機関が決定する。監督機関は必要な範囲を超えていると判断される場合、第19、20条により、意見提示及び勧告などの是正措置をとる。それによって、過大な保有を防止することができる。また個人情報ファイルを保有している長は新規ファイルの保有、変更、廃止等の場合、行政自治部長官にあらかじめ通報し、各機関別に散在している個人情報現況を把握し、これを公告しなければならない(第6条、7条)。このような公告は行政自治部長官が年1回官報に掲載することになっているが、それによって、個人の情報がどの機関で処理されているのかを知らせ、国民の閲覧、訂正請求の機会を与えている(第7条)。第8条は、個人情報保有機関長は個人情報台帳を作成し、一般人が閲覧できるようにしている。

第9条においては、個人情報の流出、盗難、紛失、変造、毀損を防止するよう、安全性確保条項を設けている。第10条は、他機関における処理情報の利用及び提供を制限している。但し、情報主体の同意、他法律の定める所管業務の遂行、情報主体の明白な利益がある場合、犯罪捜査と控訴の提起及び維持に必要な場合、法廷の裁判業務を遂行するために必要であると判断される場合はその例外として制限されない。

(4) 個人の権利保障

第12条1項は、公共機関が保有する個人情報の本人による閲覧請求権を認め、また同条2項は請求があった場合に、第13条が定める閲覧制限事由に該当しない限り、情報保有機関の長がそれを本人に閲覧させる義務を負うことを定めている。制限事由としては、①租税徴収、教育等の分野において、情報を閲覧させることで「当該業務の遂行に重大な支障を招く場合」および②「個人の生命・身体を害する恐れがあったり、個人の財産とその他の利益を不当に侵害する恐れがある場合」があげられている。

また第14条1項は、本人による処理情報の訂正請求権を認め、また同条2項は請求があった場合に、情報保有機関の長が、遅滞なく調査し

必要な措置をした後、その結果を請求人に通知する義務を負うことを定めている。

第15条は、閲覧および訂正請求に対して行政機関の長のとった処分、不作為、によって権利利益の侵害が生じた場合の、行政不服審判請求権を認めている。

これら条項は、自己情報コントロール権を認めた部分でもある。またそれ以外にも抹消、漏洩、不当目的使用者、不正閲覧については第23条～25条において罰則規定を設けている。

(5) 指導監督体系 (図3参照)

(a) 個人情報保護審議委員会

個人情報保護委員会は国務総理所属機関であり、行政自治部次官を委員長とする(第20条)。委員会は個人情報保護に関する政策及び制度改善に関する事項、処理情報の利用及び提供に対する公共機関間の意見調整に関する事項、その他大統領令が定める事項を扱う審議機関である(第20条1、2、3項)。委員は学界、言論界、法曹界、関連団体及び関係部所公務員(行政自治部、法務部、情報通信部、国家情報院)等、9名であり、委員長の推薦で国務総理が任命・委嘱し、その任期は2年である(施行令第27条)。

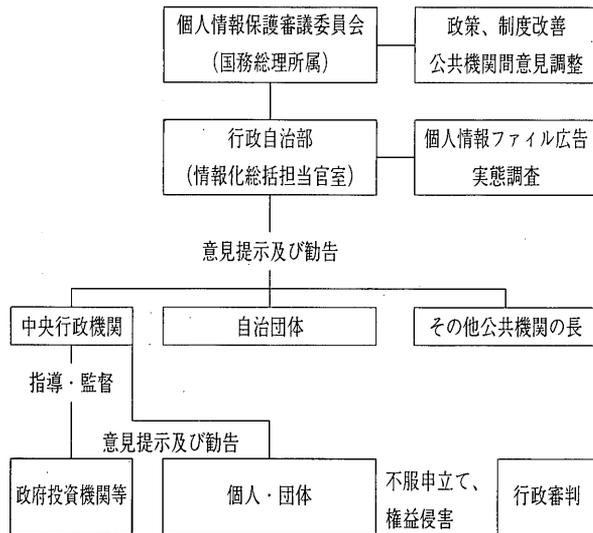
(b) 行政自治部長官

行政自治部長官は公共機関の長に対して個人情報処理に関する資料の提出を要求する権限と所属公務員に対して実務調査を命じる権限を持つ(第18条)。また公共機関の長に個人情報保護に関して意見を提示、勧告する権限をも持つ(第19条)。資料提出要求の対象機関は個人情報保護を保有する全ての公共機関であり、その期間は30日以内である。実態調査対象は個人情報保護制度運営に関する全般事項である。意見提示及び勧告は違法・不当な法運営で、私生活の侵害あるいはその恐れがある場合である。

(c) 中央行政機関の長

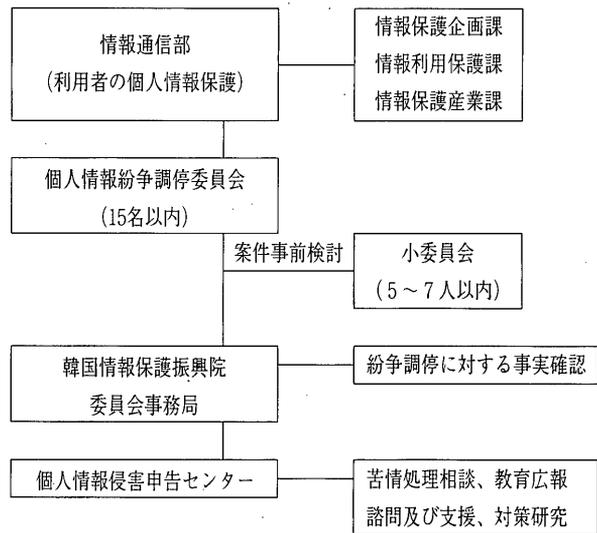
中央行政機関の長は中央行政機関傘下公共機関に対する資料提出要求、実態調査、一般監督行使権を持つ(第21条)。また個人情報保護に必要な場合には個人・団体に対しても勧告権を持つ(施行令第26条)。

〈図3〉 公共機関の個人情報保護体系



出典：行政自治部『公共機関の個人情報保護制度の理解と解説』8頁より

〈図4〉 民間部門の個人情報保護体系



出典：行政自治部『公共機関の個人情報保護制度の理解と解説』9頁より

2. 民間部門の個人情報法制（情報通信網利用促進等に関する法律）

憲法第17条は公権力に対して直接効力を持つが、私人との関係においては間接効力を持つにとどまるので、民法の不法行為、刑法の名誉毀損等による解決に頼らざるをえない。したがって、私人間の個人情報侵害が急増する情報化社会において、民間部門を規律する法律の存在は必要不可欠である。

現在、インターネット上で個人情報保護を規律する代表的な法律は「情報通信網利用促進及び情報保護等に関する法律」である（以下情報通信網⁽²⁸⁾法）。この法律は民間部門の個人情報保護において一般法的性格をもつ。民間部門に適用される法律は各分野別、つまり、電子取引、電子署名、信用取引、証券取引などその適用範囲を限定したものが存在するが、それらは情報通信網法に優先して適用される特別法の地位をもち、該当法律の規定が不備な場合は情報通信網法が補充的に適用される（図4参照）。

情報通信網法はOECDの個人情報保護8原則⁽²⁹⁾を受容すると共にEUの個人情報保護指針を考慮し、1999年制定、2000年1月1日に施行されたが、2001年12月31日に一部改正が行われ、2002年7月1日から施行されている。

(1) 情報通信網利用促進等に関する法律の主要構成内容（本文9章67条、附則）

第1章 総 則

目的、定義、他の法律との関係、情報通信網利用促進等に関する施策講究

第2章 情報通信網の利用促進

第3章 電子文書仲介者を通じた電子文書活用

第4章 個人情報の保護

第1節 個人情報の収集

個人情報の収集、個人情報の収集制限等、

第2節 個人情報の利用及び提供

個人情報の利用及び提供等、個人情報処理の委託、営業譲受等の通知、個人情報管理責任者の指定、個人情報の保護措置、個人情報の破棄

第3節 利用者の権利

利用者の権利等、法定代理人の権利、損害賠償、

第4節 個人情報紛争調停委員会

個人情報紛争調停委員会の設置及び構成、委員の身分保障、委員の除斥・忌避・回避、紛争の調停、資料要請等、調停の効力、調停の拒否及び中止、調停手続

第5章 情報通信網での青少年保護等

第6章 情報通信網の安定性確保

第7章 国際協力

国際協力、個人情報関連国際契約の制限

第8章 補 則

資料提出等、権限の委任・委託、秘密維持等、情報通信サービス提供者以外の者に対する準用、韓国情報通信産業協会、罰則適用における公務員擬制

第9章 罰 則

罰則、両罰規定、過料

(2) 目的及び適用対象

この法律は情報通信網利用を促進し、情報通信サービスを利用する者の個人情報を保護すると共に情報通信網を健全・安全に利用する環境を造成することによって国民生活の向上と公共福利の増進に報ずることを目的とする（第1条）。

適用対象は情報通信サービス提供者（電気通信法第2条第1項第1号による電気通信事業者と営利目的で電気通信役務を利用し情報を提供・媒介する者）、情報通信サービス提供者により個人情報を提供された者、個人情報の収集・管理を委託された者（第58条）、ホテル、旅行社、塾・教習所等情報通信サービス提供者以外の者を適用対象とし（以上は観光振興法第3条1項の規定によるオフライン事業者であり、施行令第28条により準用される）、スパムメール防止規定は営利目的の広告性情報を伝送する全ての国民を適用対象としている。

この法律で保護される個人情報は紙、ディスク、コンピュータ、インターネット等、個人情報が流通される方法とは無関係に全て適用される。

(3) 個人情報の収集

情報通信サービス提供者は利用者の個人情報を収集する場合、利用者の同意を得なければならない（利用者同意の原則、第22条）。但し、情報通信サービス利用契約の履行に必要な場合、情報通信サービス提供による料金精算のために必要な場合、この法律あるいは他の法律に特別な規定がある場合はそうではない（第22条但書）。また、収集に対する同意を受けようとする場合にはあらかじめ個人情報管理責任者の姓名・所属部署・職位及び電話番号その他連絡先、収集目的及び利用目的などを告知するか約款に明示することを義務化している（第22条2項、OECD個人情報保護指針の目的明確化原則、公開

の原則）。

情報通信サービス提供者は情報通信サービスの提供に必要な最小限の情報を収集しなければならないが、必要最小限の情報以外の個人情報を個人が提供しないという理由でサービス提供を拒否してはならない（必要最小限の収集原則、第23条）。同条は思想・信念・過去の病歴等個人の権利・利益及び私生活を顕著に侵害する恐れのある個人情報の収集をも禁止している（第23条）。但し、利用者の同意があるか他の法律に収集上個人情報が明示されている場合はそうではない（第23条1項但書）。この条項はEUの個人情報保護指針にいう敏感な情報の収集禁止とOECD個人情報保護指針の収集制限の原則と同趣旨で設けられている。

(4) 個人情報利用及び利用提供と個人情報管理責任者

情報通信サービス提供者は当該利用者の同意がある場合、情報通信サービスの提供による料金精算のために必要な場合、統計作成・学術研究または市場調査のために必要な場合として特定個人を見知ることができない形態で加工して提供する場合、他の法律に特別な規定がある場合を除き、個人情報の収集当時告知した範囲または情報通信サービス利用約款に明示した範囲を越して利用するか第三者に提供してはならない（第24条第1項）。また、情報通信サービス提供者から利用者の個人情報を提供された者は当該利用者の同意があるか他の法律に特別な規定がある場合を除き個人情報を提供された目的外の用途でこれを利用するか第三者に提供してはならない（第24条第2項）。

個人情報サービス提供者は個人情報管理責任者を指定し、利用者の個人情報を取り扱う者を最小限で制限しなければならない（第24条第3項、第27条第1項）。そこで個人情報を取り扱う最小限の者は、利用者を直接相手にしてマーケティング業務を遂行する者、個人情報管理責任者等個人情報管理業務を遂行する者、その他業務上個人情報の取扱が不可避な者であると定められている（指針第10条）。個人情報管理責任者は利用者の個人情報を取り扱う際、紛失・盗難・漏出・変造・毀損されないよう安全性確

保に必要な技術的・管理的措置を講究しなければならない（第28条）。また、個人情報の収集目的あるいは提供目的を達成した場合には当該個人情報を破棄するよう規定している（第29条）。利用者の個人情報を扱うか扱った者は職務上知ることのできる個人情報を毀損・侵害または漏らしてはならない（第24条第4項）。これを違反した場合は5年以下の懲役あるいは5千万ウォン以下の罰金に処される。付け加えて、第54条において情報通信サービス提供者が個人情報保護規定に違反する事項を内容とする国際契約を締結することを禁止し、国家間個人情報の収集・利用などにおいても国際基準が受容された情報通信網法規定を守ることを規定している。

(5) 個人情報処理の委託

情報通信サービス提供者等が他人に利用者の個人情報の収集・取扱・管理などを委託する場合には書面、電子メール、電話、ホームページを通じて予めその事実を利用者に告知しなければならない（第25条第1項）。委託された者も委託により個人情報を収集する際には予め委託された事実を当該情報主体に告知しなければならない（指針第12条第4項）。第25条1項の規定によって情報通信サービス提供者等から個人情報の処理の委託を受けた者は当該業務と関連して発生した損害賠償責任に限り情報通信サービス提供者等の所属職員とみなされる（第25条第2項）。この規定は民法第756条の使用者責任規定が適用されることを定めた部分である。したがって、委託者である情報通信サービス提供者が選任・監督上の過失がないことを立証すれば免責される。しかし、まだ免責を認めた判例はないこともあって、事実上無過失責任を負っていると解される⁽³⁰⁾。

(6) 営業の譲受等の通知

情報通信サービス提供者等が営業の全部または一部を譲渡するか合併・相続などでその権利・義務を移転する場合、営業の全部または一部の譲渡、合併または相続等の事実と情報通信サービス提供者等の権利・義務を承継した者の姓名（法人である場合法人の名称）、住所、電話番号その他連絡先をインターネットホームページに最小30日以上掲示するか、情報通信サービス

利用者に対して書面、電子メールその他の方法でその旨を通知しなければならない（第26条第1項、施行令第11条第1項）。

情報通信サービス提供者等から営業の全部または一部を譲り受けているか合併・相続などで情報通信サービス提供者等の権利・義務を承継した者も情報通信サービス提供者等の権利・義務を承継した事実及び該当の情報通信サービス提供者等の姓名、個人情報管理責任者の姓名・所属部所・地位及び電話番号その他連絡先、個人情報の利用目的、個人情報収集・利用及び提供に関する同意撤回、個人情報の閲覧あるいは訂正要求など利用者の権利・及び行使方法、個人情報項目、個人情報保有期間及び利用期間などに関する事項を上述した方法により利用者に通知しなければならない（第26条第2項）。

情報通信サービス提供者が営業譲受・譲渡・合併の時、利用者に個人情報移転事項の事前同意を得ることは現実的に事業者の大きな負担になり、そのため、これらの場合、利用者に対する事前同意ではなく、通知を義務化するだけに行っている。これは個人情報の第三者移転時の同意規定の例外として認められている部分である。

(7) 利用者の権利

利用者は個人情報の収集・利用及び提供においていつでも同意を撤回することができる（第30条第1項）。自己情報に対する閲覧を要求し、エラーがある場合はその訂正をも要求することができる（第30条第2項）。また、第30条第3項・4項の規定により、利用者の同意撤回、閲覧、訂正要求があった場合は遅滞なく必要な措置を講究しなければならない。エラーの訂正を要求された場合は訂正するまで当該個人情報を提供あるいは利用してはならない（第30条第5項）。満14歳未満の児童からの個人情報収集・利用の場合、法定代理人の同意を得ることを規定している（第31条）。加えて、個人情報保護規定違反で損害があった場合、立証責任は情報通信サービス提供者にあり、その立証責任が転換すると規定している（第32条）。

(8) 個人情報紛争調停委員会

個人情報に関する紛争を調停する機関であり（第33条）、訴訟外的紛争解決機関（ADR）に

該当する。委員会は委員長1人を含め15人以内の委員で構成されその内1人は常任にする（第33条2項）。委員は大学や公認された研究機関で助教授以上またはそれに相当する職にあるかあった者として個人情報保護関連分野を専攻した者、4級以上の公務員またはそれに相当する公共機関の職にあるかあった者として個人情報保護業務に関する経験がある者、判事・検事または弁護士の資格がある者、情報通信サービス利用者団体の役員の職にあるかあった者、情報通信サービス提供者または情報通信サービス提供者団体に役員の職にあるかあった者で構成される（第33条第3項各号）。委員は情報通信部長官が任命あるいは委嘱し、任期は3年である（第33条第4項、第5項）。

紛争調停対象は個人情報に関する全ての紛争である。その具体的類型を見てみると①事業者が利用者の同意なしに個人情報を収集、②個人情報を特性人が盗用、侵害、毀損、③情報主体の同意ない第三者への個人情報提供、④事業者の過大な個人情報要求、⑤加入したサイトで会員脱退ができない、⑥事業者の個人情報閲覧、訂正要求に応じ、⑦紛争相手の過多あるいは過少な補償、賠償要求により発生した紛争などがある⁽³¹⁾。

個人情報侵害の被害者は誰でも調停を申請することが可能であり、利用者のみならず、事業者もそれを行うことができる。委員会は調停に先立って両当事者間の合意を勧告する。合意勧告により合意が成立すると事件は終了するが、合意が成立しなかった場合、調停手続が開始される。調停手続が進行すると当事者の意見聴取、証拠収集、専門家の意見聴取など必要な手続を取って60日以内に双方に適当な調停案を提示し、受入を勧告する。この場合、事件の申請者や相手は委員会の会議に参加して自分の意見を開陳することができる。調停手続進行中、円満な合意が成り立つなどの事由によって調停が必要でなくなった場合、申請者は調停申込を撤回することができる（第36条2項）。

個人情報紛争調停委員会の調停を通じて下された決定に対して、調停決定日から15日以内にその当事者は受諾可否を通報しなければならない

（第38条2項）。当事者が受諾し、調停書に記名捺印した場合は調停が成立する（第38条第4項）。この場合、第38条第4項により、両当事者間には調停書と同一な内容の合意（民事上の和解契約）が成立されたとみる。

紛争調停委員会は紛争の性質上、紛争調停委員会で調停することが適当ではないと認めるか不正な目的で申請されたと認められる場合には、調停を拒否することができる。この場合調停拒否の事由などを申請者に知らせなければならない（第39条）。紛争調停委員会は申請された調停事件に対する処理手続の進行中、一方当事者が訴を申し立てた時には、その調停の処理を中止してこれを当事者に知らせなければならない（第39条第2項）。

(9) 韓国情報保護振興院

政府投資機関であり、公法上の財団である。健全な情報通信秩序の確立及び情報の安全な流通のために情報保護に必要な政策、制度及び技術を研究開発することで情報化促進に尽くすことをその任務としている。個人情報保護のため振興院内に個人情報侵害申告センターを運営している⁽³²⁾。

(10) 個人情報侵害申告センター

個人情報申告センターは情報通信網法上の個人情報保護規定が履行されているかを監視し、技術的諮問その他の支援、個人情報侵害に関連した苦情処理及び相談、個人情報侵害と関連対策研究、個人情報侵害防止のための教育及び広報、その他上の業務に付随される事業等を遂行する（施行令第26条）。

個人情報申告センターには誰でも個人情報が侵害された場合申告することができる。また、個人情報に関連した事項等の相談を受けることもできる。受理された事項は情報通信部調査計画により当事者を調査し、法規違反可否を決定する。違反事項の程度によっては過料賦課及び捜査が依頼され、その措置結果を申告者に通報する⁽³³⁾。

3. 個人情報保護マーク制度

インターネットを通じる電子商取引の利用が広がる一方で、個人情報の侵害、無断流出、売買な

ど被害事例も増加している。したがって、インターネット利用者の個人情報効果を効果的に保護し、安心してオンライン取引ができる信頼基盤構築が必要になった。その必要性に応じて、インターネットサイトの個人情報保護政策及び管理水準を総合的に客観的に評価して一定基準を満たした場合、個人情報保護優秀サイト認証マーク（ePRIVACYマーク）を付与する制度を取り入れた。合せて、ePRIVACYマーク取得業社が海外でも個人情報保護優秀サイトで認証受けられるようにするために2002年2月には日本経済産業性傘下日本情報処理開発協会のプライバシーマークと国際相互認定のためのMOUを締結した。⁽³⁴⁾

申込対象はインターネットサイトを通じて個人情報を収集、取扱、管理する国内事業者及び一般人（団体）であるが、申込日3ヶ月以内に個人情報関連法律違反で過料賦課及び刑事処罰を受けた事業者（運営者）は対象から除かれる。

認証基準は情報通信網利用促進及び情報保護等に関する法律、個人情報保護指針、個人情報保護指針、韓国情報通信産業協会インターネットサイト安全マーク審査基準を根拠に、7分野59項目（必須17項目）で構成される。審査分野は個人情報の収集に関する措置、個人情報の利用及び管理、利用者の権利、公開及び責任、満14歳未満の児童に関する特別措置、利用者権利救済等である。

マーク付与の期待効果として、個人情報不法取引及び侵害などインターネット利用者の不安要素を予防して電子商取引が促進され、民間の自律的な個人情報保護管理体系の定着でe-Business信頼文化が定着し、海外マークと相互認定を結ぶことで国内事業者の海外利用者の拡充及び市場進出の支援が進むこと等が挙げられる。⁽³⁵⁾

4. 韓国における個人情報保護法の課題

以上、韓国における個人情報保護現況を公共部門と民間部門に分けて述べた。以下は公共部門と民間部門におけるいくつかの課題を提示する。

まず公共部門における問題は、第一にコンピューターによって処理される個人情報だけを保護した（第1条）点である。⁽³⁶⁾これは行政側の便宜性だけを考慮した規定ではないだろうか。手記情報を保護するには、行政庁の負担も大きいであろう。

しかし手記データも一般に保護価値が否定されるものではなく、また多くの国は手記データを保護対象としている。⁽³⁷⁾

第二に例外条項による法適用限界の克服である。第6条と第10条がその例である。第6条は公共機関の長が個人情報ファイルを保有しようとする時、行政自治部長官に事前に通報しなければならないことを定めている。しかし例外として国家の安全、外交、犯罪捜査、その他国家の利益に関連する場合などを定めている。処理情報の利用及び提供の制限を定めている第10条においても、個人情報の保有目的以外の利用と提供を制限しながら、第6条と同様の例外規定を設けている。公共機関の都合により個人情報保護の原則に逆らう機会を与えた規定であるとの感がする部分であり、その改善が求められる。

第三に個人情報保護審議委員会制度の改善である。個人情報審議委員会は最近5年間で1回しか会議を行っていないなど単純審議機構にすぎないという批判もある。⁽³⁸⁾そのため、このような委員会を監督する独立した監督機構を設置するか個人情報審議委員会の機能を強化することが必要である。公共部門の個人情報保護審議委員会や民間部門の個人情報紛争調停委員会などは各々国務総理、情報通信部に所属し、侵害処理の公平性に劣るとされている。⁽³⁹⁾また公共部門の個人情報保護体系は図3で見たとおり、権益侵害による行政審判以前の救済手段が空白で、救済手続が不十分である。

民間部門においては、第一に法適用の複雑性の改善である。情報通信網法は民間部門における一般法的役割を期待して制定されたが、各部門別に法律が散在し、法適用に複雑性をもつ。個人情報の侵害形態は医療、信用情報など複合的になりことが多い。散在する関連規定を統合する必要性の声も上がっている。⁽⁴⁰⁾第二に自律規制活性化のための努力である。個人情報マーク制度はよく活用されれば個人情報侵害を事前に防げる一歩前進した制度であるが、実際マーク取得業者はあまりにも少ない。その活用のため、より活発な広報活動が必要であろう。第三に適用範囲を拡大する必要性がある。現行法はオフライン事業者の場合、ホテル、旅行者、塾・教習所を施行令第28条により準用してその対象とするが、それ以外は情報保護の

死角地帯である。その拡大が要求される⁽⁴¹⁾。第四に調停制度の改善である。個人情報紛争調停委員会は資料提出要求権及び施政要求権の権限がなく、紛争の実質的解決には難関が多い。また調停案に記名捺印したときに合意が成立したとみると規定されている（第38条）が、調停が成立してもそれは当事者の約定の効力に過ぎなく、その執行のためには訴訟が必要とされる問題がある。したがって、調停には当該紛争に関する裁判上の和解の効力を認めたほうがいいとの意見もある⁽⁴²⁾。

5. 小括

4では韓国における個人情報保護法の課題をいくつか挙げたが、それ以外にも課題や問題は数多く残っている。韓国の個人情報保護法は情報化促進という政府の目標と個人情報侵害問題の調和の過程から生じた法律であり、個人情報そのもの、あるいはプライバシー保護だけを考慮して定められたものではないからであろう。個人情報が行政側の効率性、企業の利益と対等あるいは優越した地位を得るためには、社会全般にわたって、個人情報保護の重要性についての認識の広まりが必要なのである。他方、個人情報を利用する側にも相応の責任が求められる。さらに法制定と改正に先立って、政府には社会全般の個人情報に対する認識向上のための持続的教育・広報活動が要求される。

現在、上記諸委員会は行政部の一部になっている。しかし国家による情報の収集・監視情報の非対称性は、権力の肥大化という危険につながる。権力分立・基本的人権の保障を害する要因を監視し、統制する役割を果たすためには、国家から独立性をもつ監督機関の設立が不可欠であると考えられる。

国家の個人情報過多収集による権力集中・監視問題は以下「Ⅲ. 電子住民カード」「Ⅳ. 教育行政情報システム」のパートで論ずることにする。
(未完)

註

- 1 金チョルス『憲法学概論』（博英社・2000）522頁、成樂寅『憲法学』（法文社・2001）409頁参照
- 2 『2002個人情報保護白書』（情報通信部）24～25頁

- 3 権寧星『憲法学原論』（法文社・2003）424頁
- 4 権寧星『憲法学原論』（法文社・2003）427頁、洪性邦『憲法学』（玄岩社・2002）450頁
- 5 本件判決の背景については鄭宗燮「韓国の民主化と憲法裁判所」大久保史郎・除勝編『現代韓国の民主化と法・政治構造の変動』（日本評論社・2003）78頁
- 6 通信政策研究所『世界のプライバシー法』（1987）23～25頁参照
- 7 本件判決については <http://www.jucl.net/web/frame03714d.html>も参照
- 8 権寧星『憲法学原論』（法文社・2003）425頁、崔大權『憲法学講義』（博英社・1998）262頁
- 9 国家は、科学技術の革新と情報及び人力の開発を通じて、国民経済の発展に努めなければならない
- 10 金チョルス『憲法学概論』（博英社・2000）519頁。同教授のとる憲法第10、17条の理解については金哲洙『韓国憲法の50年』（敬文堂・1998）105頁以下も参照。
- 11 金チョルスは憲法第10条の性格を、憲法第10条が「全ての国民は人間としての尊厳と価値を持ち、幸福を追求する権利を持つ」という点で天賦人権即ち、前国家的自然権を宣言したと見ている。また、第10条「国家は個人が持つ不可侵の基本的人権を確認しこれを保障する義務を負う」と定められているところは不可侵・不可譲の前国家的基本権を憲法上宣言することで実定法上の保障をしていると考えている。憲法第10条が前国家的自然権を実定法化したことはこれを一般的に公布することで生活により強い強行力を付与し、執行力を付与することでその実効性を保障するためであると解している。（金チョルス『憲法学原論』（博英社・2002）257頁）
- 12 悠久な歴史と伝統に輝く私たち大韓国民は3・1運動で建立された大韓民国臨時政府の法統と不義に抗拒した4・19民主理念を受け継いで、祖国の民主改革と平和的統一の使命に立脚して正義・人道と同胞愛として民族の団結を強固にして、すべての社会的弊習と不義を打破し、自律と調和を土台に自由民主的基本秩序をもっと確固にして政治・経済・社会・文化のすべての領域において各人の機会を均等にし、能力を最高度で発揮できるようにして、自由と権利による責任と義務を果すようにし、中では国民生活の均等な向上を期して外では恒久的な世界平和と人類共栄に貢献することで我々と我々の子孫の安全と自由と幸福を永遠に確保することを念におしながら1948年7月12日に制定され8次にかけて改正になった憲法をここに国会の議決を経て国民投票によって改正する。1987年10月29日
- 13 大韓民国は統一を指向し、自由民主的基本秩序に立脚した平和的統一政策を樹立してこれを推進する
- 14 ①政党の設立は自由であり、複数政党制は保障される。②政党はその目的・組織と活動が民主的でなければならず、国民の政治的意思形成に参与するのに必要な組織を持たなければならない。③政党は法律が決めるところ

- により国家の保護を受け、国家は法律が定めるところにより政党運営に必要な資金を補助することができる。④ 政党の目的や活動が民主的基本秩序に違背される時には政府は憲法裁判所にその解散を提訴することができ、政党は憲法裁判所の審判により解散される。
- 15 成樂寅『憲法学』（法文社・2001）
- 16 学説の整理は金鐘鐵『韓国憲法上の自己情報コントロール権と知る権利の憲法的根拠』「ノモス」2002年12月号335頁参照
- 17 許堂『韓国憲法論』（博英社・1998）363頁
- 18 許堂『韓国憲法論』（博英社・1998）516頁
- 19 権寧星『憲法学原論』（法文社・2003）432～433頁、金チョルス『憲法学概論』（博英社・2000）529頁
- 20 権寧星『憲法学原論』（法文社・2003）433頁
- 21 個人情報侵害申告センターの個人情報具体的項目は <http://www.cyberprivacy.or.kr>
- 22 柳煌彬『デジタル時代の個人情報保護技術』64～65頁
- 23 情報の非対称性（information asymmetry）：企業はクッキーなどを活用して、個人の情報を数多く、正確に保有していて、他の企業にも売っている。しかし、個人は自分に関する情報を誰が、どの企業が、どのぐらい持っているか流通されているのかを知ることは困難である。
- 24 柳煌彬「情報化時代の個人情報保護方案研究」『インターネット法律』第4号2001年84～88頁
- 25 趙晟容「韓国における個人情報の刑法的保護」クレジット研究27号269頁以下参照
- 26 民願とは、国民（「民願人」）が行政機関に対し処分など特定の行為を要求する行為をいう。
- 27 本法の日文訳は園田寿氏による <http://www.lawschool-konan.jp/sonoda/korea/law/hogo.html>を参照。また同法解説は申九賢「韓国のプライバシー・個人情報保護法」堀部政男編『情報公開・プライバシーの比較法』（日本評論社・1996）も参照。
- 28 同法の日文訳は園田寿氏による <http://www.lawschoolkonan.jp/sonoda/korea/law/riyou-new.html>を参照。
- 29 ①収集制限の原則（COLLECTION LIMITATION PRINCIPLE）②データ内容の原則（DATA QUALITY PRINCIPLE）③目的明確化の原則（PURPOSE SPECIFICATION PRINCIPLE）④利用制限の原則（USE LIMITATION PRINCIPLE）⑤安全保護の原則（SECURITY SAFEGUARDS PRINCIPLE）⑥公開の原則（OPENNESS PRINCIPLE）⑦個人参加の原則（INDIVIDUAL PARTICIPATION PRINCIPLE）⑧責任の原則（ACCOUNTABILITY PRINCIPLE）
- 30 『2002個人情報保護白書』（情報通信部）47頁
- 31 <http://www.e-privacy.or.kr>
- 32 <http://www.kisa.or.kr>
- 33 <http://www.cyberprivacy.or.kr>
- 34 デジタルタイムス2002年2月28日記事参照
- 35 <http://www.privacymark.or.kr>
- 36 もっとも第1条のかかげる立法目的とは別に、同法は「個人情報」を手記データを含む広い概念として用い、それについては第4条で「最小限の範囲での収集」の原則、第9条で収集した情報の安全確保義務を定めている。ただしこれら「（コンピュータによって）処理」されていない個人情報については、同法12条ないし15条の保護は及ばないと解される。
- 37 鄭英和『情報社会のプライバシー保護のための政策課題』プライバシー保護ネットワーク第1次定期討論会文20頁
- 38 電子新聞2004年3月10日記事参照
- 39 オマイニュース2003年8月19日、2003年12月17日記事参照
- 40 ハジョンヒョン『個人情報制度のジレンマと効果的な導入法案』 <http://www.kisa.or.kr/edu/essay99/index.htm>
- 41 白允哲『憲法上個人情報自己決定権に関する研究』法曹2002.5178頁
- 42 崔正烈『インターネットと個人情報保護』41頁（2002年7月6日韓国情報法学会第6次シンポジウム（第3分科）「新技術の登場と個人情報」）。本文は、<http://www.kafil.or.kr>（韓国情報法学会ホームページ）を参照。