



---

# 研究レポート

---

No.268 June 2006

---

---

個人情報保護法の施行に伴う介護事業者の課題

主任研究員 渥美由喜

上級研究員 瀧口樹良

---

富士通総研（FRI）経済研究所

研究レポート

# 個人情報保護法の施行に伴う 介護事業者の課題

2006.3.27

## 【要旨】

1. 2005年4月に、個人情報の適切な取り扱いを事業者等に義務づける「個人情報保護法」が全面施行された。介護業務では、他の業務と比べて多くの個人情報を扱うのみならず、個人のプライバシー度も高い個人情報（センシティブ情報）を取り扱うという特徴があるが、大半の介護関連事業者における個人情報保護の対応は、遅れているようである。
2. そこで本論では、保護法および厚生労働省ガイドラインのポイントと問題点、および介護事業者に求められる対策などについて、実際にどのような個人情報をどう取り扱うべきか、従来の守秘義務との違い、法により明文化されるさまざまな義務、セキュリティ対策の重要性などについて検討を行った。
3. 個人情報保護法の施行を契機として、事業者、介護サービスに従事する者の双方にとって、「倫理コンプライアンスの確立」が最優先すべき課題である。

主任研究員 渥美由喜  
atsumina@jp.fujitsu.com  
上級研究員 瀧口樹良  
takiguci@jp.fujitsu.com

## 目 次

1. はじめに	3
2. 個人情報保護法とは	4
2.1 保護法制定の背景	4
2.2 世帯単位の福祉制度と個人単位の保護法	8
3. 介護事業者における「個人情報」	9
3.1 保護法および厚労省ガイドラインの具体的な内容	9
3.2 保護法、厚労省ガイドラインの対象者	9
3.3 福祉情報システムの概要	9
3.4 医療・介護情報の発生源と個人情報	11
4. 介護におけるプライバシーと個人情報保護	13
4.1 介護情報の特殊性と利用課題	13
4.2 介護におけるプライバシーと個人情報保護	13
4.3 秘密保持に関する患者の権利	13
4.4 介護における個人情報保護の基本的考え方	14
5. 介護事業者が直面するリスク	15
5.1 介護事業者が直面する罰則リスク、訴訟リスク、信用喪失リスク	15
5.2 プライバシー情報の保護	15
5.3 漏洩リスクの危険性	16
5.4 「個人データの第三者への提供」と「安全管理措置」の重要性	18
5.5 第三者認証制度の事業者取得の急増	21
6. 今後の課題と具体的な対応策	23
6.1 倫理コンプライアンスの確立	23
6.2 具体的な対応策	23

## 1. はじめに

2005年4月に、個人情報の適切な取り扱いを事業者等に義務づける「個人情報保護法」が全面施行された。これにより、多くの民間事業者が適応を受けることとなり、当然ながら介護事業者などにも同法が適用される。

介護業務では、他の業務と比べて多くの個人情報を扱うのみならず、個人のプライバシー度も高い個人情報（センシティブ情報）を取り扱うという特徴がある。したがって、介護事業者が取り組むべき課題は大きいといえる。また、保護法施行に伴い情報漏洩リスクが高まる可能性もあり、その対策は急務である。しかしながら、介護関連事業者に対する個人情報保護の対応は、遅れているようである。

そこで本論では、保護法および厚生労働省ガイドラインのポイントと問題点、および介護事業者に求められる対策などについて、実際にどのような個人情報をどう取り扱うべきか、従来の守秘義務との違い、法により明文化されるさまざまな義務、セキュリティ対策の重要性などについて検討を行い、提言するものである。

## 2. 個人情報保護法とは

### 2.1 個人情報保護法制定の背景

個人情報の保護は、我が国特有の課題ではなく、国際的に取り組まれている課題である。というよりは、むしろ、欧州などにおけるプライバシー保護等の先進的な取り組みにおける考え方が、我が国の個人情報保護法に大きな影響を与えている。つまり、我が国の個人情報保護法はヨーロッパからの輸入品という側面がある。

そこで、個人情報保護に関する国際的な取り組みや、わが国におけるこれまでの取り組みを通じて、個人情報保護法成立の背景について確認しておきたい。

#### 2.1.1 国際的な個人情報保護の取り組みの原点（OECD 8原則）

1970年代、コンピュータにより大量の個人情報が処理されるようになると、プライバシーに関する関心が高まり、ドイツ、フランスといった欧州の数カ国において個人情報保護に関する法律が成立されるようになった。しかしながら、各国が個人情報の保護に関してまったく違った法律やガイドラインを持っていたために、国際的ビジネスなどの場で多くの問題が発生した。

そこで、1980年、OECD（経済協力開発機構）は、各国が満たすべき個人情報保護のレベルを一定にするためのガイドラインを策定し、このガイドラインに従って自国の制度を整えていくことになった。これが「プライバシー保護と個人データの国際交流についてのガイドラインに関する理事会勧告」である。

OECDは、この勧告において、「プライバシーの保護」と「情報の自由な流通の確保」という、競合する2つの価値観の調和を目的として、いわゆる「OECD 8原則」を示し、加盟各国に対して、国内法制にこれを反映させることを求めた。

この「OECD 8原則」とは、次の8つの原則から成っている。

##### (1) 収集制限の原則(Collection Limitation Principle)

個人データは、適法かつ公正な手段によって収集されるべきである。収集にあたっては、データ主体（本人）に知らせるか、または同意を得るべきである。

##### (2) データ内容の原則(Data Quality Principle)

個人データは、その利用目的に沿ったものでなければならず、かつ、利用目的に必要な範囲内で正確、安全であり、細心なものに保たなければならない。

##### (3) 目的明確化の原則(Purpose Specification Principle)

なぜ個人データを収集するのか、その目的を事前に明確にしておく必要がある。個人データの利用は、収集目的の達成に必要な範囲内に限られなければならない。

#### (4) 利用制限の原則(Use Limitation Principle)

個人データは、第 3 原則（目的明確化の原則）によって明確にされた目的以外の目的のために開示・利用、その他の使用に提供されるべきではない。ただし、「①データ主体（本人）の同意がある場合」、「②法律の規定による場合」はこの限りではない。

#### (5) 安全確保の原則(Security Safeguards Principle)

個人データは、紛失、不正なアクセス、破壊などの危険に対して、合理的な範囲内で安全に保護されなければならない。

#### (6) 公開の原則(Openness Principle)

個人データが存在していること、利用目的、個人データの管理者名、データ管理者の住所などが、容易に入手できる必要がある。

#### (7) 個人参加の原則(Individual Participation Principle)

個人は、次の権利を有する。

- ①データ管理者が自己に関するデータを有しているか否かについて、データ管理者またはその他の者から確認を得られること。
- ②自己に関するデータを下記の形で知らせること。
  - i) 合理的な期間に
  - ii) もし必要なら、過度にならない費用で
  - iii) 合理的な方法で
  - iv) 自己に分かりやすい形で
- ③上記①及び②の要求が拒否された場合には、その理由が与えられること及びそのような拒否に対して意義を申し立てることができること。
- ④自己に関するデータに対して意義を申し立てること、及びその意義が認められた場合には、そのデータを消去、修正、完全化、補正させること。

#### (8) 責任の原則(Accountability Principle)

データ管理者は、上記の諸原則を実施する責任を有する。

この「OECD 8 原則」は、後述する EU 指令や我が国の個人情報保護法においても、その基本的考え方が採用されるなど、その後の世界各国の個人情報保護法制度に大きな影響を与えるものとなった。

### 2.1.2 欧州における個人情報保護の取り組み

欧州では、EU 統合の進展に伴い、情報が EU 域内で国境を越えて自由に移動することを確保する必要性から、1995 年に「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 EU 指令」(EU 指令)を採択した。この EU 指令は、先ほど確認した「OECD 8 原則」を実現する構成となっている。

EU 指令自体には法的拘束力はないが、EU 加盟各国は EU 指令にもつづき国内法を整備する義務を負っている。このため、EU 加盟各国は、この指令に基づいて国内法制を順次整備してきた。ただし国によって、裁判制度などその基盤となる制度が異なっていたり、事前規制（届出、登録制度）を行っている国もあるなど、各国によりその対応は異なっている（図表 1）。

図表 1. EU 加盟各国の個人情報保護の取り組み

国名	動向
イギリス	2000年3月 1998年データ保護法 施行
フランス	検討中
ドイツ	2001年5月 連邦データ保護法 施行
ベルギー	2001年9月 個人データの処理に係るプライバシー保護法 施行
デンマーク	2000年7月 個人データの処理に関する法律 施行
スペイン	2000年1月 個人データの保護に関する法律 施行
ギリシャ	1997年4月 個人データの処理に係る個人の保護に関する法律 施行
イタリア	2000年5月 個人データの処理に係る個人及び他の主体の保護に関する法律 施行
ルクセンブルク	2000年10月 法草案を議会に提出
オランダ	2001年9月 個人データ保護法 施行
オーストリア	2000年1月 2000年データ保護法 施行
ポルトガル	1998年10月 個人データ保護法 施行
フィンランド	1999年6月 個人データ保護法 施行
スウェーデン	1998年10月 個人データ保護法 施行

(出所) 岡村久道、新保史生 (2002)

### 2.1.3 米国における個人情報保護の取り組み

米国における個人情報保護法に関する制度は、公的（行政）分野と民間分野で異なっている。公的分野については、プライバシー法（1975年9月施行）により規制されているが、民間分野については、基本的に自主規制により個人情報の保護を行うとして、包括的な法律は制定されていない。ただし、特に個人情報保護が重要な特定の分野に関しては、個別法により規制する方法をとっている。個別法としては、「公正信用取引法」「ケーブル通信政策法」「ビデオプライバシー法」「子どもオンラインプライバシー法」などがある。

ところで、前述した EU 指令の中には、十分な個人情報保護のレベルを実現していない第三国への EU 各国からの個人情報の移転を禁止する条文を各国法に求めるという「第三国条項」が含まれている。このため、自主規制に任せている米国は、EU 側からみると、十分な個人情報の保護レベルを実現していない第三国であると判断される可能性がある。そうすると EU から米国への個人情報の移転ができないことになり、航空券の国際線予約などさまざまな場面で支障を来すことになる。

そこで、米国商務省は 1999 年、EU 指令と同レベルの「セーフハーバー原則」を作成し、「セーフハーバー原則」の遵守を自ら宣言した米国の事業者においては、EU と同水準の個人情報の保護がなされているとみなすこととした。この「セーフハーバー原則」にもとづき、EU とアメリカは 2000 年にセーフハーバー協定を締結、EU からの個人情報の移転を認めることとなった。

#### 2.1.4 我が国における個人情報保護の取り組み

わが国においても、情報化の進展により、個人情報の保護が重要な課題として注目されるようになってきた。また、国際的にも、前述したように 1980 年に「OECD 8 原則」が発表され、この内容を反映した国内法制の整備が急務となってきたため、国の行政機関を対象とした「行政機関の保有する電子計算機にかかわる個人情報保護に関する法律」が制定された。

しかしながら、その後、個人情報の流出や漏洩などの事例が次々と明らかになり、社会問題化するケースが出てきたことから、民間分野も対象とした個人情報保護の必要性が強く認識されるようになった。その結果、1999 年 6 月に、「住民基本台帳法改正法案」の審議過程で、「個人情報保護に関する法律について法制化を図る」旨の与党合意が成立した。

このような経緯から、1999 年 7 月、当時の高度情報通信社会推進本部の下に個人情報保護検討部会が設置され、民間分野をも対象とした個人情報保護に関する法整備を速やかに整えるとの観点から、政府全体として、個人情報の保護・在り方を総合的に検討することとされた。同年 11 月には、個人情報保護検討部会が「わが国における個人情報システムの在り方について（中間報告）」を発表、2000 年 1 月には、高度情報通信社会推進本部の傘下に、個人情報保護法制化専門委員会が設置された。2000 年 6 月に、個人情報保護法制化専門委員会は、「個人情報保護基本法制に関する大綱（中間報告）」を、11 月には「個人情報保護基本法制に関する大綱」をそれぞれ発表した。また、住民基本台帳ネットワーク制度が 2002 年 8 月 1 日にスタートすることとなり、個人情報保護法はこの制度の安全面での裏付けにもなっているため、制定がより急がれることとなった。

こうした流れを受けて、2001 年 3 月、第 151 回国会に「個人情報の保護に関する法律案」が提出されたが、法案中の「基本原則」の条項が抽象的すぎたために、解釈の仕方によっては国家権力によるメディアの規制に利用される可能性があるなどの意見が出され、マスコミや野党がこぞって反対した。その結果、この法案は継続審議が繰り返されたものの、

2002年12月の臨時国会において審議未了で廃案となったのである。

そこで政府与党は、メディア規制につながる可能性があるとの理由で特に反対が多かった「基本原則」の条項を削除するなどして、第156回国会に法案を再提出、2003年5月23日、「個人情報の保護に関する法律」（以下、「個人情報保護法」と呼ぶ）が成立した。

個人情報保護法は、大きく分けて2つのパートからなっている。1つは、わが国の個人情報保護法に関する基本的な考え方を示す基本法にあたる部分であり、もう1つは、民間事業者に対する規制にあたる部分である。基本法にあたる部分は、2003年5月30日から施行され、民間事業者に対する規制にあたる部分は、2005年4月1日から施行されることとなった。

## 2.2 世帯単位の福祉制度と個人単位の保護法

次に、保護法と介護保険制度の間に横たわっている根本的な問題について指摘しておきたい。先述のように、日本における個人情報保護に対する取り組みは、あくまでも「輸入品」に過ぎない。日本社会で長く醸成されてきたものではないため、現時点では日本の諸制度とは相容れない側面もある。その1つが、社会福祉制度である。日本の社会福祉制度は、個人単位ではなく、基本的に世帯単位で設計されている。つまり、家族福祉でまかなえない部分を社会福祉で支えてきたという経緯がある。したがって、介護保険制度の仕組みにも、世帯単位が色濃く反映されている。例えば、厚生年金は会社員の時と、会社員を辞めた後の水準は、専業主婦の妻と2人で生活できるような数字になるよう、現在、約23万8,000円の水準になるように設定されている。つまり、個人が高齢時に生活する水準ではなく、夫婦2人という世帯ごとに水準が設定されている。これと同様に、社会福祉制度もまた個人単位ではなく、基本的に世帯単位が設計単位になっているという特徴がある。介護保険法は、個人単位と世帯単位が混合しており、これまで家族福祉で賄えない分を社会福祉で支えて、福祉を充実させてきた。このことから介護保険制度についても世帯単位という発想が色濃く反映されているのは当然のことである。

例えば、介護事業者が介護サービスを提供するに際しては、利用者の個人情報の範疇にはおさまらない、世帯構成員に関する情報を知っておかなければならない。このように、介護業務と個人情報保護対策には相反する要求事項がある点も注意する必要がある。保護法への対応策とは、保護法に関する知識を蓄えておけば大丈夫というレベルの問題ではない。

しかしながら、厚労省には、そのような認識が欠けているようだ。保護法の規定には、介護保険の指定基準に織り込み済みの事項も少なくないため、「激変はない」（老健局振興課）としているが、これは認識が甘いと言わざるをえないだろう。世帯単位と個人単位という根本的な違いを認識した上で、今後の個人情報保護の対応策を考えていく必要がある。

他国と比較すると、日本は、自助、共助、公助のなかで共助が強く、それを公助で支えている構成になっている。共助は、家族福祉もあれば、企業福祉も非常に手厚く、様々な

施策が講じられてきた。このような共助の面が強いのが日本の福祉の特徴である。スウェーデンの介護は、女性が自分の親を介護しても主人の親を介護することはまずない。公助に関しても、非常に個人主義が強い国である。それに対し、アメリカでは高齢になるまで一人暮らしをし、一人暮らしが難しくなったときにはボランティアに援助を受けられるので、公助システムはあまり重要でなく、低福祉低予算となっているのである。

### 3. 介護事業者における「個人情報」

#### 3.1 保護法および厚労省ガイドラインの具体的な内容

保護法とは、いわば個人情報の取扱いに関して共通する「必要最小限のルール」を定めたものである。ルールの詳細については各事業等の分野の実情に応じて、事業者が自律的に取り組むこととしている。そこで、2004年10月に厚労省の検討会は「医療・介護分野での個人情報取り扱いに関するガイドライン」をとりまとめた。

保護法において、個人情報とは「①生存する個人に関する情報であつて、氏名、性別、生年月日、その他の記述等により特定の個人を識別することができるもの、②個人の身体、財産、職種、肩書き等の属性に関して、事実、判断、評価を表すすべての情報、③映像、音声による情報も含まれ、暗号化されているか否かを問わない」と定義されている。

これに対して、厚労省ガイドラインでは、介護分野における「個人情報」として、「ケアプラン、サービス提供計画、サービス内容の記録、事故の状況等の記録等」が挙げられている。

#### 3.2 保護法、厚労省ガイドラインの対象者

では、どういう事業者が取り組むことになっているのであろうか。保護法の対象は、5,000件以上の個人情報を持っている事業者である。これに対して、厚労省ガイドラインでは個人情報保護法では対象外とされている「5,000件以下の個人情報しか持たない小規模事業者」にも法律を「遵守する努力を求める」とした点が特徴である。制度を最初に導入する際、介護保険にみられるように、最初は高いハードルを設定して、徐々に下げていき、制度を広めていく場合がある。いずれ、1,000件以下というようにハードルが下がっていく可能性が極めて高い。

これは、小規模な診療所でも情報漏洩は深刻な問題に繋がる可能性があるためであろう。医療・介護分野では、診療所や介護事業所など5,000件未満の事業者が大半を占めるが、規模の大小にかかわらず、個人情報保護のために取り組んでいく必要があることは間違いない。

#### 3.3 福祉情報システムの概要

福祉情報システムには大きく分けて、介護保険管理情報システム、要介護認定支援情報システム、介護事業者新情報システム、介護保険モニタリング支援情報システムの4つのシステムがある（図表2を参照）。こういった情報システムは、いずれも介護保険の運営上重要なシステムだが、デジタルベースによる情報システムというだけでなく、重要な管理対象個人情報を保護ガードするという意味でも重要な役割を果たしている。

図表 2 福祉情報システムの概要

システム区分	サブシステム	特 性
介護情報システム	介護保健管理情報システム	<ul style="list-style-type: none"> <li>・保険者が被保険者から介護保険料を徴収管理、介護サービス限度額を管理、介護報酬支払を管理、保険財源運営を管理などするのが目的</li> <li>・インターネットによる介護報酬請求が原則</li> </ul>
	要介護認定支援情報システム	<ul style="list-style-type: none"> <li>・要介護度の一次判定と二次判定の支援が目的</li> <li>・一次判定システムは79項目の訪問調査票を入力して判定</li> <li>・二次判定システムは要介護認定審査会業務の効率化を支援</li> </ul>
	介護事業者支援情報システム	<ul style="list-style-type: none"> <li>・施設介護サービス事業者、居住介護サービス事業者、介護支援事業者の業務支援が目的</li> <li>・施設介護サービス事業者の入所者基本管理、入所者基本管理、入退所管理介護サービス計画(ケアプラン)作成支援、介護サービス提供管理、経営管理などを支援</li> <li>・介護支援事業者のケアマネジメント、サービス事業者間調整、経営管理等を支援</li> </ul>
	介護保険モニタリング支援情報システム	<ul style="list-style-type: none"> <li>・介護保健サービスについて、事前・プロセス・事後において、サービスの質、サービス提供の妥当性、地域の介護資源の妥当性、介護報酬限度額の妥当性を検討するための継続的情報の収集・評価を支援</li> </ul>
福祉人材情報システム	(都道府県福祉人材センター)	<ul style="list-style-type: none"> <li>・福祉関係事業求人情報のDB化、福祉ボランティアのDB化のどの支援</li> </ul>

(出所) 各種資料に基づき、富士通総研が作成

### 3.4 医療・介護情報の発生源と個人情報

次に、それぞれの医療・介護施設においてどのような個人情報が発生するのかについてみていくことにする(図表3を参照)。リハビリテーション施設は様々な介護情報を持っており、利用者に関する情報はもちろん個人情報となる。他の関連施設でも、基本的には利用者情報、顧客情報はすべて個人情報となる。さらに介護福祉施設では、要介護認定情報、身体介護の情報、機能障害や日常生活動作など全て個人情報と考えられる。また、在宅医療・居宅介護施設では、利用者調査情報のほかにもサービス記録などの様々な形の記録形態があるが、これらも個人情報になる。また、介護機器製造販売をする企業でも、顧客情報が絡んでいる。また、利用者の家で、利用者そのものの情報や生活情報が発生する。行政機関も、あらゆる個人情報について、精査し取り扱いに注意している。

図表 3 医療・介護情報の発生源別分類と個人情報

その他発生源	介護情報(斜体文字は個人情報)
リハビリテーション施設	各種療法(理学療法、作業療法、言語療法など)情報、専門職(理学表奉仕、作業療法士、言語療法士など)情報、関連施設(教育施設、職業訓練施設、職業初回施設など)、他
介護福祉施設	要介護認定情報、身体介護情報、機能障害、日常生活動作(ADL)、介護・介助情報、他
在宅医療・居住介護施設	関連施設情報(訪問看護ステーション、在宅医療支援センターなど)情報、ケアプラン、サービス記録(訪問医療、訪問看護、訪問介護、訪問リハビリ、訪問入浴、通所介護、通所リハビリ、訪問入浴、通所介護、通所リハビリ、福祉用具貸与など)、サービス支援事業所情報、他
介護機器・製造・販売企業	介護機器・用具情報、市販後調査情報、介護用具保守点検情報、介護機器リース・レンタル情報、他
利用者宅	利用者様態情報、利用者生活情報、他
行政機関	各種認可情報、各種行政情報通達、人口情報、介護機器不具合情報、第三者機関監視情報、介護計画、他

(出所) 各種資料に基づき、富士通総研が作成

## 4. 介護におけるプライバシーと個人情報保護

### 4.1 介護情報の特殊性と利用課題

介護保険施設、在宅サービス事業者、居宅介護支援事業者等の介護事業者にとって、介護情報とは、介護者のケアプラン、介護サービス計画、提供したサービス内容の記録、事故状況の記録等の介護保険情報、医療・健康情報、保有資産情報、各種契約情報（介護用具レンタル等）、家族（世帯）情報である。

さらに、介護情報といっても、いくつかの次元がある。まず介護目的の利用という意味での一次利用がある。これは介護の用途で情報が利用されているという観点から、個人情報を保護するということである。ただし、一次的利用ではなく二次的内容になると、これは直接の目的とは異なるので、非常に綿密な管理をして取り扱わなければいけない義務が生じることになる。

二次的利用の一つ目は、介護情報管理のための利用である。これは介護報酬を請求する場合に、介護の質・効率の評価・安全管理のために、感染や介護事故を報告し、管理しているデータを集計・分析する必要があるからである。今後事業展開する上での検討材料として利用する際に、介護目的の利用とは違い、より厳格な基準値が適用される可能性がある。さらに、行政の利用についても同様である。また、介護研究への利用も考えられる。長期的に介護サービスを図る上では、実際の事例の取り扱いが慎重になされなければならない。

### 4.2 介護におけるプライバシーと個人情報保護

介護におけるプライバシーについて、個人情報保護として扱われる場合には、より細かく吟味する必要がある。プライバシーの概念は、個人の情報がどこにどのように存在し、どのような形で使われているかという点と関係する。20世紀前半までは、どの国においても単に個人的な事情で秘密を守るという守秘義務がプライバシーのすべてであった。ただその後、こういった守秘義務に加え、個人情報が多様なところで利用されることになり、人が意識せずに発言したり行動したりしているものを、他人が記録しホームページなどの様々な形で情報提供することは、コントロールできない状況となっている。20世紀後半以降このような情報についても個人がコントロールする権利があるのではないかという観点からプライバシー概念が拡大してきている。

また、介護情報は、極めて個人のプライバシー度が高い個人情報（センシティブ情報）を取り扱う事が多く、他の事業者に比べて、もしこうした個人情報が漏洩したときの事業者に対する信頼の低下や社会的影響の大きさは計り知れないものがあるといえる。

### 4.3 秘密保持に関する患者の権利

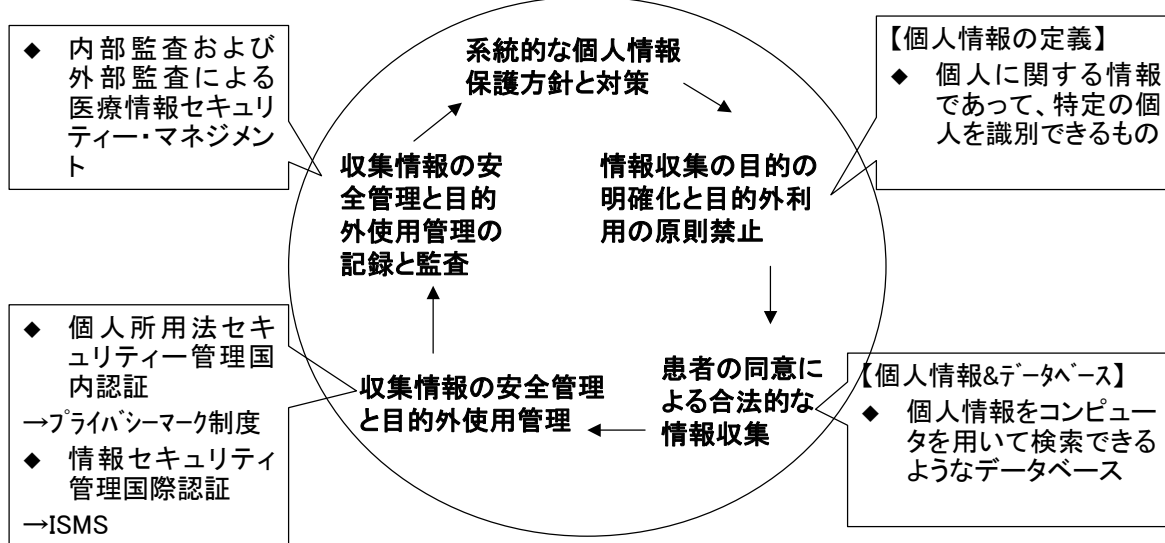
プライバシーに関して、介護利用者に適用した海外の事例はない。しかし、これに近い

ものとして、医療分野での患者の権利に関する「リスボン宣言」がある。「患者のプライバシー権利宣言（リスボン宣言）」において、患者の個人情報の秘密は死亡後でも守らなければならないとされた。ただし、患者の子孫が自らの健康上の危機に関する情報を知る権利は例外に認められている。また、患者の特定可能なデータは保護されなければならない。データの保護は、その保存形式に応じて、適切に処理することとされており、これにはコストがかかる。日本の個人情報保護法では、個人情報は生存中のみに効力があり、死後も個人情報が守られる「リスボン宣言」は、極めて厳格な基準といえる。

#### 4.4 介護における個人情報保護の基本的考え方

個人情報保護を行なうにあたり、まず体系だった方針がなければならない（図表 4 を参照）。まず、情報収集の目的が必ず明確にされなければならない。個人情報が明確に定義されないと、個人情報として特定の個人を識別できるという基準ができない。さらに、患者ないし利用者の同意による個人的な情報収集がなされると、コンピュータを用いて検索できるようなデータベースが基本的には作られるということになる。このときに、安全管理上、情報が意図していない形で将来的に使用されないかどうか管理して、記録に残し、適宜監査をしなければならない。これには、安全管理と目的外の使用管理があるが、この点については個人所有法セキュリティ管理の認証システムとして、プライバシーマーク制度がある。さらに、情報セキュリティの管理の面でも、情報セキュリティ管理国際認証（ISMS）がある。それをチェックする外部監査ないし内部監査するものとして、医療情報セキュリティ・マネジメントというものも存在する。こういったものを活用することにより、会社は個人情報保護を管理していることを外部へ明らかにすることができる。

図表 4 介護における個人情報保護の基本的考え方



(出所) 各種資料に基づき、富士通総研が作成

## 5. 介護事業者が直面するリスク

### 5.1 介護事業者が直面する罰則リスク、訴訟リスク、信用喪失リスク

企業が保護法の施行により受ける影響は、大きく二つある。一つは、保護法違反を理由に行政から改善命令が下されたり、処罰されるリスクである。例えば、これまでは個人情報の収集時には目的を通知・公表しなくてもよかったのに対して、今後は行政から処罰を受ける。

もう一つは、個人情報を漏洩させた場合、利用者から訴訟を起こされるリスクである。例えば、大手エステティックサロン TBC は、WEB サイトからの問い合わせや身体のサイズなどの個人データ約 4 万件が流出した事件に関連して、被害者グループから総額 1000 万円を超える訴訟を起こされている。京都府宇治市は、住民基本台帳のデータ約 21 万件を流出させた事件に関連して住民 3 人から訴訟を起こされ、最高裁から一人当たり 1 万 5 千円の損害賠償を支払うように命じられている。

上記二つのリスクに加えて、介護事業者には介護サービス特有の「信用喪失リスク」がある。介護サービスは「地域密着型の対人サービス」という特徴を持つため、仮に個人情報が漏洩した場合、利用者の口コミで不祥事は瞬時に広がってしまい、業績悪化に直結しかねない。仮に、処罰リスクや訴訟リスクがなかったとしても、信用損失率は非常に大きいと考えられる。地域密着型の対面サービスにおいては、こうした個人情報漏洩や、それが仮に 5,000 人以下だったとしても、その利用者の口コミで、あそこは情報がきちんと管理されてないといった悪い評判が立つと、その不祥事は、その地域において瞬時に広がってしまい、その業者のこれまで培ってきた信用を一瞬にして壊してしまい、業績悪化に直結しかねないという問題がある。

### 5.2 プライバシーの保護

介護分野のプライバシーの保護に関しては、個人の健康維持や回復にかかわる極めてデリケートな情報を扱うことから、取り扱いに細心の注意が必要である。判例では、保護されるべきプライバシーは、以下の 3 つの要件を満たす必要がある。

一つ目は、私生活上の事実に関する情報である。二つ目は、社会一般の人々の感受性を基準として、その情報が開示されると当該個人に心理的な負担や不安を覚えるため、開示を欲しないと考えられる情報である。三つ目は、一般の人々にまだ知られていない情報である。

こういった三つの要件をみると、介護事業者が取り扱う情報の多くがプライバシーに該当することになる。仮に利用者や家族のプライバシーが漏洩されたことによって、裁判沙汰になり争点になるのは、やはり精神的なダメージである。精神的なダメージを与えた場合、不法行為責任を問われる場合もある。なお、この不法行為責任は制定法によるものではなく、民事判例上の概念であり、今後裁判が蓄積されていかないと作られない法である。

今後、個人情報の漏洩に関連した判例が蓄積されていくと、プライバシーの侵害に関する不法行為責任についても定まっていくものの、それには10年近くを要すると考えられる。他方で、厚生労働省等の対応方針はいまだ不明確であり、保護法の施行後も紆余曲折が予想される。このような状況の中、介護事業者がその個人情報保護の理念や、介護制度の仕組みの違いを踏まえた上で、自主的にコントロールしていかなければならない。

### 5.3 漏洩リスクの危険性

保護法では、個人情報を取得する場合に、利用目的の通知や公表を行ったり、本人の同意がなかったりした場合には第三者への提供を禁止している。本人が求める場合は原則開示することも義務づけられている。仮に、主務大臣の命令に違反した場合は、最高6カ月以下の懲役か30万円以下の罰則が科される。

介護保険では、指定基準でサービス担当者会議等で利用者の情報を使う場合、あらかじめ文書で利用者の同意を得ることが定められている。このため、老健局振興課は「扱いに特別な変更はない」としている。

しかしながら、保護法の施行により、個人情報の取り扱いに変更はないとしても、取り扱いの要注意度、逆のいい方をすれば漏洩リスクの危険性は急速に高まると考えておいた方がよいだろう。最近、新聞記事になっている情報セキュリティに関する事件では、必ずといっていいほど漏洩した会社が恐喝されている。介護ビジネスは典型的な地場産業であるため、社会的信用を失うことは競争力を失うことにつながりかねない。そこに目をつけ、個人情報保護法を盾にとりて漏洩事業者を恐喝するといったような事件が呼び起こされる危険性は高い。

付け加えて懸念されるのは、介護事業者の情報漏洩事件は、決して少なくないという点である（図表5を参照）。NPO法人の日本ネットワークセキュリティ協会(JNSA)がまとめた「2003年度情報セキュリティ・インシデントに関する調査報告書」（2004年6月）によると、個人情報漏洩事件の多かった業種TOP8に「医療・福祉」が入っている。今後、介護事業者は早急に個人情報保護への対応を図らないといけない。

図表5 医療・介護関連の情報漏洩事故例

No.	新聞掲載日	場所・漏洩数	要旨
1	平成15年2月18日	江戸川区住民健康診断データ（病歴含む）9万人分流出	平成6年、東京都江戸川区が保管していた住民健康診断データ9万人分が流出した事件。
2	平成15年3月20日	長野県赤十字血液センター献血者1300人分の個人データ流出	センターによると、血液者登録作業をしていた派遣社員が、夫が経営するエステティックサロンの顧客名簿作りに使用。同センターは前年12月発覚後未

			報告。
3	平成15年7月3日	群馬県藤岡市社会福祉協議会などから個人データの入ったPC盗難	同市によると、2日「パソコン等盗難事件対策本部」を発足。再発防止対策（各課、諸金庫人のパスワード入力徹底、二重、三重、のセキュリティ機能、公開・非公開文書の区別の見直し、1日1回処理・保存など）を決定し全庁に通知。
4	平成15年7月15日	千葉県内7病院の看護師2244人の個人情報記録したFD盗難	東京海上火災保険によると、同社千葉支社職員が、千葉県内7病院の看護師個人情報を記録したFD入り鞆を、千葉県内で帰宅途中に車上荒らしにより盗難。
5	平成15年8月30日	高知県立安芸病院、平成13年度眼科入院カルテ100人分紛失	同病院によると、同年2月保存のための製本作業中に紛失に気づいた。カルテ保管庫に廃棄用個人情報を置いたのが原因と発表。
6	平成16年3月17日	金沢医科大学電子カルテ・パスワード漏洩	同大の助手、研修医ら8人が同大学病院患者の電子カルテにアクセスするパスワードを、指導する学生に教えていた。同大学では、平成12年7月から電子カルテを導入し、学生用電子カルテのチェックのため、主治医の電子カルテ情報を開示していたパスワード不正使用を禁じた学内規定に抵触。
7	平成16年3月24日	奈良県立三室病院（三郷町）約7500人分患者らの個人情報入りノートPC5台盗難	同病院では、看護師採用内定21人、在宅療法機器貸出情報476人、職員情報386人、職員人事関係情報101人、高度医療情報6391人などの個人情報を記録したのノートPC5台が盗難。盗難防止対策の強化、個人情報の保管・管理体制の強化を検討。
8	平成16年5月26日	鳥取県立個性病院（倉吉市東昭和町）個人情報入りレントゲンフィルムなどを産廃業者が紛失	同病院によると、同病院が処分した個人情報入りレントゲンフィルムなどを産業廃棄物業者が紛失。同権では、県立2病院のほか同様に処分していた県内44病院に対し、個人情報穂と条例を順守させることを明らかにした。県情報システム管理要綱に基づいた「情報セキュリティ対策喜寿」を独自に製作する。

9	平成16年5月22日	三重県松坂市民病院患者約15人分、職員約400人分の個人情報流出	同病院によると、前年6月頃患者約15人分の氏名、生年月日、病名、病状などが書かれた医師用会合資料200枚、医師、看護師、事務職員など職員400人分の給与額が記載された資料約10枚が流出。同病院の清掃・ごみ処理の委託業者社員から個人情報流出の通報があり返却。内記では会合資料はシュレッダー処分となっている。
10	平成16年9月18日	国立病院機構大阪医療センター患者500人分個人情報入りノートPC盗難	同センターによると、センターの机の上にあった医師のノートPC2台が盗難。PCには、がんサポートチームの対象患者ら約50人分、消化器科の患者ら約45人分のデータが入っていた。

(出所) 日本ネットワークセキュリティ協会 (JNSA) (2004) の他、各種新聞等

#### 5.4 「個人データの第三者への提供」と「安全管理措置」の重要性

では、具体的に、どのような個人情報保護の対応策を講じるべきなのだろうか。一言でいえば、個人情報に関するマネジメントシステムを確立し、自らを律しつつ、顧客（利用者・家族・関連機関）に接するといった対応が求められる。

厚労省ガイドラインでは、事業者の責務として、「①個人情報の利用目的の特定、②利用目的の通知、③個人情報の適正な取得、個人データ内容の正確性の確保、④安全管理措置、従業者や委託先の監督、⑤個人データの第三者提供の制限、⑥本人などの求めに応じた情報開示や訂正、利用停止」の6項目を示している。

このうち、「個人データの第三者への提供」は、「世帯と個人という設計単位の相違」により、介護業務と個人情報保護の目的が対立しかねないという意味において、最も重要な点である。介護業務における個人データの第三者への提供は、本人同意が原則となる。ただし、法令に基づく場合、および生命、財産保護のために必要で重度痴呆や意識不明など本人の同意を得ることが困難である場合は、同意がなくても病状などを家族に説明できるとしている（図表6を参照）。

図表 6 「個人データの第三者への提供」に関する制限

<p>第三者提供制限の仕組みについて（第 23 条）</p>	<p>個人情報取扱事業者から第三者への情報提供には、あらかじめ本人の同意が必要となる。</p> <p>例外として、届出、通知などの法令に基づく場合、急病の場合などの人の生命、身体又は財産の保護に必要な場合、疫学調査などの公衆衛生・児童の健全育成に特に必要な場合、税務調査に協力する場合などの国等に協力する場合などがあげられる。また本人の求めにより原則として提供停止（オプトアウト）することとしている場合などにおいても制限が加えられることとなっている。</p>
<p>本人の求めによる提供停止（オプトアウト）の仕組み（第 23 条第 2 項）</p>	<p>具体的事例として、住宅地図業者（表札を調べて住宅地図を作成し、販売（不特定多数への第三者提供））やデータベース事業者（ダイレクトメール用の名簿等を作成し、販売）などがある。オプトアウトの要件は、以下の 4 項目をあらかじめ通知し、又は本人の知り得る状態においている場合。①第三者に提供すること、②提供される情報の種類、③提供の手段、④求めに応じて提供停止することで、これらの要件を満たしている場合に限り、本人の同意がなくても第三者提供を容認する。</p>
<p>第三者に当たらない場合（第 23 条第 4 項）</p>	<p>委託先への提供（委託元に管理責任）は、例として、データの打ち込みなど、情報処理を委託するために個人情報を渡す場合や、百貨店が注文受けた商品の発送のために、宅配業者に個人情報を渡す場合がある。なお、個人情報取扱事業者には、委託先に対する監督責任が課せられる。合併等に伴う提供（当初の目的の範囲内）は、例として、合併・分社化により、新社会に顧客情報を渡す場合や、営業譲渡により、譲渡先企業に顧客情報を渡す場合がある。なお、譲渡後も、個人情報譲渡前の利用目的の範囲内で利用しなければならない。また、グループによる共同利用（共同利用する者や範囲や利用目的等をあらかじめ明確にしている場合に限る）は、例として金融機関の間で、延滞や貸倒等の情報を交換する場合や観光・旅行業など、グループ企業で総合的なサービスを提供する場合がある。なお、共同利用者の範囲、利用する情報の種類、利用目的、情報管理の責任者の名称等について、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置かなければならない。</p>

（出所）各種資料に基づき、富士通総研が作成

また、本人から個人情報取扱業者に対して、次のようなかたちで関与できることが定められている（図表 7 を参照）。

図表 7 本人の関与の仕組

利用目的の通知 （第 24 条第 2 項）	保有個人データがどのような目的で利用されているのかについて、原則として、本人に通知しなければならない。
開示（第 25 条第 1 項）	個人データは原則として、本人に開示しなければならない。なお、例外として、①本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合、②個人情報取扱業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合などがある。
訂正等（第 26 条第 1 項）	保有個人データの内容が事実でないときは、利用目的の達成に必要な範囲内において、訂正等を行わなければならない
利用停止等（第 27 条第 1 項、第 2 項）	①利用目的による制限、②適正な取得、③第三者提供の制限に違反していることが判明したときは、違反を是正するために必要な限度で、原則として、利用停止等を行わなければならない

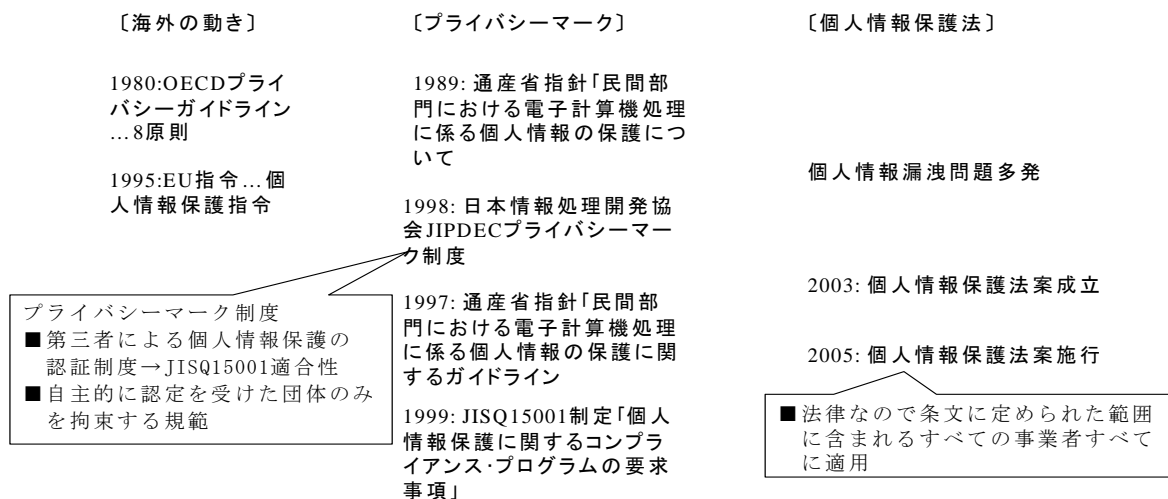
（出所）各種資料に基づき、富士通総研が作成

最後に重要なのが、「安全管理措置」である。現時点では、事業者の規模の大小で取り組みの進捗状況の差が大きいかたちとなっている。例えば、ID やパスワードを使ったデータ管理や情報保護のための推進委員会の設置などはコストがかかるため、手付かずになっている中小事業者がほとんどである。また、給付管理や請求事務を外部委託している事業者は、受託先の管理への取り組みも重要である（図表 8 を参照）といえるが、ほとんどなされていないのが実態である。



施行されている。両者の間には、基本的には関係はないが、プライバシーマーク制度は保護法よりも事業者に対して厳しい安全管理措置が求められているため、プライバシーマーク制度の認定を求める事業者が急増している。

図表 9 プライバシーマークと個人情報保護法



(出所) NPO 東京 IT コーディネータ (2004)

## 6. 今後の課題と具体的な対応策

### 6.1 倫理コンプライアンスの確立

今後、介護事業者にとって、どのような個人情報に関するマネジメントシステムが必要であろうか。事業者の中には、情報管理ということで IT コンサルタントに依頼しているケースも見られるが、IT コンサルタントはコンピュータのセキュリティに重点を置きがちになるという欠点がある。実際には大半の介護事業者は紙媒体で、顧客情報をキャビネットに施錠保管・管理しており、電子データは介護保険料請求のみというのが一般的である。従って、コンピュータ上のセキュリティ管理だけでは十分ではない。

前述した JNSA の調査によると、情報漏洩の原因は、「誤動作、設定ミス」といったコンピュータ関連の原因の他に、「内部犯罪、情報持ち出し、盗難」という人間に関連した原因があり、現在ではこの面からの漏洩事件が多発している。

### 6.2 具体的な対応策

個人情報保護の観点からは、次のような取り組みが必要不可欠なものとなる。

まず、第一に、介護スタッフには入所時にオリエンテーションと個人情報保護の同意書を提出してもらうことである。介護スタッフは資格を取得する際に、個人情報保護の教育を受けているものの、さらにプライバシー保護への意識を向上させるために、定期的な研修も必要であろう。ヘルパーは、退職など移動が激しいために、退職後の守秘義務も大切である。

第二に、介護業務は、介護利用者の利便性向上のため、情報開示が必要な部分もある。そのため、利用者との介護契約書では、守秘義務と第三者への情報開示同意書をとることも重要である。

第三に、委託先に対しては、委託契約書の中に守秘義務と同時に再委託の禁止、さらには委託先の監査権の確保を行い、委託元としてのコントロール権を有することが求められる。

第四に、顧客サービスの質の向上、あるいは社会的責任として、プライバシーマークを取得することを検討することも必要であろう。

このように、保護法の施行を契機として、事業者、介護サービスに従事する者双方にとって、「倫理コンプライアンスの確立」が最優先すべき課題となっている。こうした課題に対して、積極的に取り組むかが、介護事業者の将来性を大きく左右することとなるであろう。

(参考文献)

- ・渥美由喜 2005a 「個人情報保護法対策の手引き 世帯単位の社会福祉制度と根本的な違いを認識したうえで対応策を考えていくべき」日本医療企画『介護ビジョン』2005年2月号、pp34-38
- ・渥美由喜 2005b 「漏えい事件が多い「医療・福祉事業」判例が蓄積されるまで 紆余曲折を重ねる可能性も」日本医療企画『介護ビジョン』2005年3月号、pp45-49
- ・渥美由喜 2005c 「個人情報保護法と介護サービスにおけるリスクマネジメント」(社)かながわ福祉サービス振興会会員向け特別講演
- ・日本ネットワークセキュリティ協会(JNSA) 2004 「2003年度情報セキュリティインシデントに関する調査報告書」
- ・岡村久道、新保史生、2002 『電子ネットワークと個人情報保護 ーオンラインプライバシー法入門ー』経済産業調査会
- ・東京 IT コーディネータ 2004 「NPO 東京 ITC による P マーク取得支援について」