堀部政男情報法研究会
第8回シンポジウム

2013年9月1日

企業から見たわが国の個人情報保護法制の「有効性」と行政手続番号法

関西大学　社会安全学部・大学院社会安全研究科
教授・博士（法学）　高野一彦

Graduate School and Faculty of Safety Science FSS © Kazuhiko.Takano

1．問題意識

2012年1月20日 欧州委員会「特に技術発展に焦点をあてた、新たなプライバシーの課題への異なるアプローチの比較研究（以下「ECプライバシー研究報告」）」における、ニューサウスウエールズ大学のグレアム・クリーンリーフ教授の調査結果「Country Studies B.5–Japan」におけるわが国の評価

「データ保護の「十分性（adequacy）」を充足していると判断することは困難」

その根拠として「私企業にとっては、法律違反による多額の罰金や集団訴訟よりも、風評リスクによる損害（risk of reputational damage）のほうが重要」であり、わが国の法律が、「有効」であるとの根拠を見いだせない、との指摘。

EUデータ保護の「十分性」の基準

（1）「個人データの第三国への移転：EUデータ保護指令25条及び26条の適用の実務文書」「ルールへの優れたレベルのコンプライアンス」があることが要件
Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 24 July 1998

（2）オーストラリアの2000年プライバシー修正（民間部門）法の欧州委員会への認定申請
第29条作業部会の意見では主に法制度の外形的要件と執行状況の評価
Article 29 Data Protection Working Party Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000, (5095/00/EN WP40 final) Adopted on 26th Jan. 2001」

グリーンリーフ論文では「有効性（effectiveness）」を重く見ている

新プライバシー保護法制の潮流

2012年1月25日　EU一般データ保護規則提案
同年2月23日　　アメリカ消費者プライバシー権利章典
2013年5月24日　個人情報保護3法の特別法としての「行政手続き番号法」成立
：
マイナンバー法に採用された「世界レベル」のプライバシー保護

・独立性が高い監視機関の設置
・情報の不正取得への刑事罰
・プライバシー影響評価の実施と運用、マイポータルなど

※「国際的にも通用する強度」（堀部政男一橋大学名誉教授）との評価

今後・・・
・「番号法」における特定個人情報保護委員会の設置と人事
・医療等個人情報保護委法案の議論は収束

個人情報保護法の改正へと議論が発展？

新たなデータ保護法制の研究は、遵守する企業のコンプライアンス研究と一体となり、「有効性」を担保する制度設計が必要ではないか

2. 企業から見た「有効性」

（1）株式会社の類型による違い

会社法　⇒　大会社及び委員会設置会社の「内部統制システム構築義務」

大会社及び委員会設置会社の取締役には**内部統制システム構築義務**がかかっている。体制整備の内容は会社法施行規則 100条1項「業務の適正を確保するための体制」に、**使用人のコンプライアンス体制（4号）**について、**企業グループとしての体制の構築を親会社等の取締役の義務（5号）**と規定している。

株主代表訴訟、第三者訴訟

金融商品取引法　⇒　有価証券報告書提出会社の「内部統制報告義務」

金融商品取引法において、**有価証券報告書提出会社**に**「内部統制報告制度」が義務**付けられている。その具体的な内容は、金融庁「財務報告に係る内部統制の評価及び監査の基準」および「同実施基準」に規定されており、**「全社的な統制」**として**リスク管理体制に関する自己評価を行い、外部監査人の内部統制監査**を受け、内閣総理大臣に報告書を提出する義務を負う。

内部統制報告書の**虚偽記載**への刑事罰・罰金

大会社及び委員会設置会社、有価証券報告書提出会社（公開会社）の経営者にかかる法的義務は、コンプライアンス経営を促すモチベーションとなっている

（2）企業法務におけるリスク評価の問題

① 個人情報保護法における主務大臣の権限の行使

主務大臣による「勧告」「命令及び中止命令」至る可能性は低い

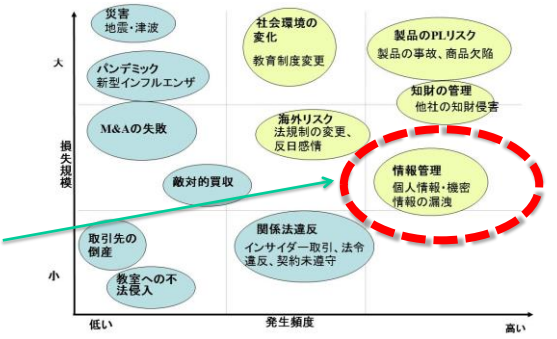
	苦情相談	漏えい事案	勧告、命令及び中止命令	備考
H23年度	5,267件	420件	0件	報告の徴収16件、助言1件
H22年度	6,212件	413件	0件	報告の徴収15件

出所：消費者庁「平成23年度個人情報の保護に関する法律施行状況の概要」2011年9月、43頁。

② 訴訟リスク

数多くのプライバシーの権利の侵害に関する判例が存在するが、おおむね賠償額は、数千～数万円の間。侵害行為への抑止力としての効果が極めて低い。

「発生頻度」と「損失規模」で優先順位をつける企業のリスク評価では、「情報法CP」の優先順位は低くなる



（3）事業形態による違い

法人顧客相手の事業と、個人顧客相手の事業では、企業のコンプライアンスへの取組みに違いが出る

個人顧客	不信を招く行為は不買運動につながり重要なリスク	適法かつ社会受容性を考慮したルール設定と運用
法人顧客	消費者の信用低下を重要なリスクと捉えない傾向	現行法制度の「間隙」をつく挑戦的なルール設定と運用

例：個人情報保護法における第三者提供の同意⇒法と社会受容性に乖離
⇒明確な同意を追及するか、約款の一条項として記載するか、など

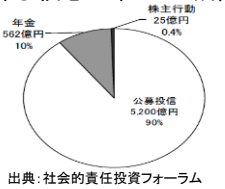
参考 社会的責任投資（Socially Responsible Investment, SRI）ファンド

米国におけるSRIの投資残高 （単位：10億ドル） 出典：SOCIAL INVESTMENT FORUM <http://www.socialinvest.org>

1995年	1997年	1999年	2001年	2003年	2005年	2007年	2009年
$639	$1,185	$2,159	$2,323	$2,164	$2,290	$2,711	$3,071

参考：国＝2400億ポンド（約45兆円、2007年）、日本＝8400億円（2009年）

伸び悩む日本のSRI残高



出典：社会的責任投資フォーラム <http://www.sifjapan.org/>

Dow Jones Sustainability Assessment Questionnaire

Economic dimension ： 32問
Environmental dimension： 31問
Social dimension： 36問
→ コーポレートガバナンス
リスクマネジメント
コンプライアンス

まとめ　ー企業から見たわが国の個人情報保護法制の「有効性」ー

根拠	義務・誘因	対象	効果
会社法	内部統制システム構築義務	大会社・委員会設置会社の取締役	株主代表訴訟、第三者訴訟による損害賠償請求
金融商品取引法	内部統制報告制度	有価証券報告書提出会社の経営者	報告書の虚偽記載に刑事罰・罰金
個人情報保護法	主務大臣による権限の行使	個人情報取扱事業者	「勧告」「命令」等 但し、近年は0件
プライバシー侵害訴訟	民事訴訟の提起	全ての法人・個人	損害賠償額は概ね数千円～数万円
[参考] CSR評価	SRIファンドのインデックスとして採用	公開会社	企業価値の上昇 日本のSRI残高は伸悩む

非大会社かつ非公開会社であり、法人顧客対象の事業を行っている企業は、
法の「有効性」を担保するプレッシャーが全くかかっていない。

小規模事業者、小資本で起業できて多額な設備投資が不要なため株式公開による資金調達の需要が少ないインターネットビジネスのような業態が該当
＝国際的にみればデータ保護ルールが最も有効に機能して欲しい分野

明確で対象を限定しない罰則の規定が必要
独立監視機関による確実な権限行使と事業者へのコンサルテーションが必要

監視機関による確実な執行と事業者へのコンサルテーション

2011年8月10日～13日　トロントを訪問（IPC Office、CHEO、Kids Media Centerを調査）

1. Information and Privacy Commissioner of Ontario
　Dr. Ann Cavoukian　⇒「Privacy by Design」提唱者

（1）Commissionerの職責

プライバシー保護と情報公開の両分野について、
独立した法執行機関として、官民双方を監視
・法の遵守監視と執行
・国民への情報提供、教育啓発、事業者の相談
・プライバシー影響評価と検査　（官民双方）など

（2）Commissionerの権限

・強制調査権＝市民からの不服申立に関する調査
・自己付託による調査、勧告、命令、訴訟提起と参加

（3）Commissioner Office

・140人のスタッフ中、約70名はプライバシー、約70名は情報公開
・行政機関との人事交流あり（情報公開担当の副委員長は行政出身）
・年間予算は約14億円（2010-11年度）、ほとんどは職員の人件費

参考：　イギリス インフォメーション・コミッショナー制度

ウイルムズローに所在、人員327人（IOCが独自採用）、年間予算は約30億（2017万£、2009-10年）

※出典：石井夏生利「英国におけるインフォメーション・コミッショナーの組織と権限」2010年8月21日、17頁。

監視機関による確実な執行と事業者へのコンサルテーション

2011年8月10日～13日　トロントを訪問（IPC Office、CHEO、Kids Media Centerを調査）

2. 事業者の意見

東オンタリオ小児病院（CHEO)のエルイーマム博士（Dr. Khaled El Emam）

オンタリオ州の新生児の登録情報のデータベースを新薬や治療後術の開発に利用
データベース構築にあたって、患者からの情報取得から研究者への情報提供の一連のスキームについて、IPCに相談してプライバシー保護の仕組みを導入し、PIAと数回の検査を経て運用

⇒「事業者にとっても時間と経費の低減につながり、相談は有益であった」
「コミッショナーによる監視と執行はオンタリオの事業者の意識を高めている」

その他、子ども向け優良サイトの認証を行っているKids Media CenteのMs. Gordonrも同意見

監督機関による監視と執行が事業者のコンプライアンス意識を高めている点は、小規模事業者やインターネットビジネスにコンプライアンス経営を促すプレッシャーが低いわが国が「有効性」を高めるための示唆

3. 企業における個人情報保護のもう一つの課題

国内法が企業に求める過剰な管理

①重層的な法制度　　個人情報保護法
個人情報保護法に基づく各省庁のガイドライン
47都道府県・1750市町村等の個人情報保護条例
JIS Q 15001（プライバシーマーク）

②個人情報＋利用目的の管理のためのデータベース構築

海外法規への日本企業の対応

EUデータ保護指令26条1項、2項及び4項の例外的措置

①情報主体の明確な同意
②標準契約条項（SCC）⇒データ保護当局の承認
③拘束的企業準則（BCR）⇒　域内3当局の承認
又は、そもそもデータを移転せずEU域内で完結

EU一般データ保護規則提案、への対応が予想される

その他、消費者プライバシー権利章典、改正OECDガイドラインへの対応も・・

わが国の会社法・金取法は海外法規の遵守も求めているため、**膨大なコストと労力**をかけて情報管理体制を構築している　（しかしEUにおけるわが国の評価は低い）

非公開の小規模事業者やインターネットビジネスとのコンプライアンス経営への取組みの格差がますます拡大する傾向

EU一般データ保護規則提案のコンプライアンス上の論点

2012 年1 月25 日　改定案を公表

「指令（Directive）」から「規則（Regulation）」へ
「規則（regulation）」は自動的に全加盟国の国内法の一部となる
⇒多国籍企業の負担軽減（標準契約条項、拘束的企業準則の承認の簡素化）

「地域的な範囲」におけるEU域外適用（3条2項）
EUデータ保護規則案は、EU域外企業であっても、① EU居住者への商品・サービスの提供、② EU居住者の行動の監視、を行っている管理者に対して適用される。

「同意の条件」における明確な同意取得（7条2項）
公表文などの中で示される場合は、区別して明示（explicit）する義務、同意撤回の権利を保障する義務を追加。（「黙示の同意」、「約款の条項」などは明示的でない）
⇒わが国の現行法制における「同意」の適法性とは異なる

「監督機関への報告」（31条）
個人データ違反を発見した場合、24時間以内に監督機関に報告する義務
⇒危機管理体制の整備

「行政制裁」（79条）
監督機関は、EUデータ保護規則に反した管理者・処理者に対して最大1,000,000ユーロ、もしくは全世界での年間売上高のうち最大で2%まで過料として科す。

その他、「データ保護ルールの遵守を確実にする役割を果たす、独立した監視機関」の設置（（41条2項(b)））を「十分性」の要件として求めていると解される。

4. 行政手続番号法における国際的整合

個人情報保護ワーキンググループは、EUデータ保護指令における保護の十分性やPbDなどの国際的な考え方、EUデータ保護指令の改正の動向に配慮
⇒個人番号及び特定個人情報等に限定した法律ではあるが、「国際的にも通用する強度」（堀部政男一橋大学名誉教授）との評価

① 監視機関　⇒　特定個人情報保護委員会

EUデータ保護指令28条の「監督機関」
・完全なる独立性は「三条委員会」の設置形態で担保
・調査権限⇒「報告及び立入調査（52条）」、
・介入権限、司法的救済権限⇒「50、51及び54条」

② 事前の検査　⇒　特定個人情報保護評価

EUデータ保護指令20条の「事前の検査」⇒「特定個人情報保護評価（27条）」

③ 制裁　⇒　罰則

EUデータ保護指令24条の「制裁」⇒67～77条に刑事罰を規定
（ただし刑法、不正アクセス禁止法等の他の法律で対応できる行為態様は除く）

個人情報保護3法の特別法であり、わが国のデータ保護の「十分性」に影響を及ぼさないが、国際的観点から十分性要件を充足する法が成立した意義は大きい

［参考］ 情報の不正取得者への法的制裁は「間隙」

わが国における情報の不正取得への刑事罰

1．情報の不正取得に対し、有体性説を有力説とする刑法の財産犯規定の適用は困難であった。

ex.大日本印刷事件東京地判昭40.6.26、京王百貨店事件昭62.9.30

2．不正競争防止法における営業秘密侵害罪は、「秘密管理性」の要件が厳しく、実効性に乏しかった。

ex.営業秘密に関する裁判例で、81件は秘密管理性の判断をしたと考えられ、肯定したものは23 件（経済産業省「営業秘密管理指針」2010年、8頁）

法的な保護を受けるために「個人情報」を「営業秘密」として管理
【例】緊急連絡名簿に、㊙と書いて金庫に保管し、鍵は部長だけが使える

企業防衛上、個人情報の不正取得への刑事罰が必要

欧米諸国との比較

営業秘密：アメリカ96年 経済スパイ法（Economic Espionage Act）
経済スパイ罪、トレード・シークレット窃盗罪の創設
ex.U.S. v. Okamoto, Serizawa(2001年)、U.S. v. Zhu, Kimbara（2002年）

個人データ：UK98年データ保護法（Data Protection Act 1998）
第55条 個人データの違法な取得等への刑事罰

5．むすびにかえて －個人情報保護法制における監督機関と罰則－

EUデータ保護指令 第24条「制裁」（Sanctions）

「加盟国は本指令の条文の完全な実行を確実にするために適切な措置を採択し、指令に従って採用された国内法規の条項の違反に対しする制裁を規定する」と規定

EU一般データ保護規則提案 第78条「刑罰」（penalties）

「加盟国は本規則の条項への違反に適用する刑罰をルールとして規定」し「刑罰は効果的（effective）で均衡が取れ（proportionate）、抑止的（dissuasive）でなくてはならない」と規定

行政手続番号法⇒刑事罰が規定⇒不正取得行為等に対する抑止力として期待。

番号法の一般法としての個人情報保護法は不正取得者への法的制裁を規定していない。
1999年10月20日「高度情報通信社会本部個人情報保護部会（堀部政男座長）」の議論で刑事罰が検討されたが見送られた。その結果・・
①主務大臣の関与の少なさと相俟って抑止力としての効果が期待できない
②EUによる「十分性」の要件を充足しない可能性
③企業防衛上の不都合⇒不競法「営業秘密侵害罪」の適用は構成要件が厳しく使えない
営業秘密としての管理が過剰反応を促進し、利用と流通を制限

一般法としての個人情報保護法の改正を検討すべきではないか。その観点は・・
①刑事罰の導入による不正取得事案の抑止効果
②独立監視機関による監視と権限の執行、事業者のコンサルテーション
⇒特定個人情報保護委員会の権限の拡大

⇒「有効性」を高める