

## 情報法制と企業のコンプライアンスに関する比較研究

著者	野 一彦
雑誌名	セミナー年報
巻	2011
ページ	1-10
発行年	2012-03-31
その他のタイトル	Current Studies Relating to Information Law and Corporation Compliance in Japan as International Comparison
URL	<a href="http://hdl.handle.net/10112/7069">http://hdl.handle.net/10112/7069</a>

# 情報法制と企業のコンプライアンスに関する比較研究\*

高野 一彦

子どもの安全とリスク・コミュニケーション研究班研究員  
社会安全学部准教授

## はじめに

本稿では、「企業保有情報保護」をテーマとして、個人情報・プライバシー保護、営業秘密保護法制に関する現代的な課題を抽出し、新たな法制度の提言を試みる。

情報のデジタル化、ICT (Information and Communication Technology ; 情報通信技術) の進展に伴い、法律学の中でも情報法への関心が高くなり、社会制度として情報保護法制の定立と整備への期待が高まっている。堀部政男 (1981) は、情報法を、「情報に特有な法現象を総体としてとらえる場合、これを「情報法」と呼び、また、情報法に関する学問的研究を法律学の一分野に位置づけるならば、これを「情報法学」と称することができる<sup>1)</sup>」と定義し、その後発展を遂げてきた。

しかし、わが国の個人情報・プライバシー保護法制は欧州諸国から約 30 年遅れて成立したが、EU (European Union : 欧州連合) からは「十分なレベルの保護」とは評価されていない。また営業秘密の不正取得への刑事罰はアメリカから数年遅れて導入されたが、国際的な不整合を抱えている。これらは企業における国際間の様々なコンフリクトの原因になっており、結果として経済障壁になっている。

そのような中、政府・与党社会保障改革検討本部は、2011 年 1 月 31 日「社会保障・税に関わる番号制度についての基本方針―主権者たる国民の視点に立った番号制度の構築―」(以下、「政府の基本方針」という。)を公表した。この中では、2015 年に共通番号制を導入するとともに、第三者機関を含む新たな法制度を施行することが規定されている。政府の基本方針に基づき、同本部は「社会保障・税番号大綱―主権者たる国民の視点に立った番号制度の構築―」を公表し、新法制の定立による社会保障・税に関わる番号制度の導入、および第三者機関の設立

---

\* 本稿は、2011 年 5 月 18 日に開催された関西大学経済・政治研究所第 190 回産業セミナーにおける報告に執筆・修正を加え、2012 年 1 月 28 日に脱稿したものである。

1) 堀部政男「情報法」『法と政策』1981 年 12 月号 (第一法規、1981 年)

に関する大綱を示した。今後、新法の施行に伴い、第三者機関をどのような制度に設計するのか、また個人情報保護法との整合をどのようにとるのか、などの議論がすすむことが予想される。

このように、わが国の情報法、とりわけ個人情報・プライバシー保護法制、および営業秘密保護法制は変革の過程にあり、わが国が抱える課題を解決するために欧米諸国の法制度との比較研究を行い、わが国の新たな情報法制を提言する絶好の機会であろう。

## 1 欧州によるわが国のプライバシー保護の評価

欧州各国では、1970年代にデータ保護法制が相次いで制定された。スウェーデン（1974年データ法）、西ドイツ（1977年連邦データ保護法）、フランス（1978年データ処理・ファイル及び個人の諸自由に関する法律）、イギリス（1984年データ保護法）などである。欧州諸国のなかには、法律条文上、個人データの国外処理を制限する条項を設ける国があり、その利害関係の調整から国際的なデータ保護の基準が必要になった。

1995年10月24日、欧州会議及び理事会は「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1995年10月24日の欧州議会及び理事会の95/46/EC指令（以下、「EUデータ保護指令」という。）<sup>2)</sup>」を採択した。本指令は、プライバシーの保護と個人データの自由な流通の確保を目的とし、公共部門と民間部門の双方における、個人データの自動処理、または一部のマニュアル処理に適用される。

EUデータ保護指令第25条第1項では、「加盟国は、処理されている、又は後に処理される予定の個人データの第三国への移動は、当該第三国が適切なレベルの保護を提供している場合に限られることを規定するものとする。但し、本指令に従って採択された国内規定に対する遵守を害しないことを条件とする。」<sup>3)</sup>と規定している。EU域外諸国においても同レベルのデータ保護施策を講じさせることを企図し、構成国は、第三国が「十分なレベルの保護」（adequate level of protection）を確保している場合に限ってデータの移転を行うことができることを定めなければならないとしている。

この規定は、EU構成国以外の国にとって重要な規定である。「十分な保護措置」であると評価されるためには、わが国の代表による公式な要請を欧州委員会に提出し、EUデータ保護指令第29条作業部会（Article 29 Working Party）による評価を行い、欧州委員会が最終判断を

---

2) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 31995L0046, Official Journal L281, 23/11/1995 P. 0031-0050.

3) 電子商取引実証推進協議会ECOM、プライバシー問題検討ワーキング・グループ「電子商取引における個人情報の保護に関する中間報告書」の参考資料の和訳を引用した。

行うという手続きを踏むことになる。しかし、「十分な保護措置」の基準は公表されていない。EUデータ保護指令第25条第2項において「あらゆる状況にかんがみて」評価することとしており、必ずしも要求レベルが具体的ではない。

EUによるわが国のプライバシー保護に関する評価は決して高くない。2009年4月23日、ベルギー・ブリュッセルで行われたデータ保護会議（BJA-Conference on Data Protection）において、欧州委員会関係者が行ったプレゼンテーションの中で、「日本は、個人の私生活にかかわる個人データ及び基本権に関して十分なレベルの保護を提供している国であるとは、EUによってまだ考えられていない。」<sup>4)</sup>と述べたと紹介されている。

EUデータ保護指令第25条第1項の規定は、わが国企業のグローバル化に多大な影響を及ぼしている。たとえばEU構成国に所在する企業が、わが国に個人データを移転する場合は、EUデータ保護指令第26条1項、2項および4項に設けられた例外的措置を利用することになる。

EUデータ保護指令第26条第1項では、「データの対象者が提案された移転に対して、明確な同意を与えている」場合、「移転がデータの対象者と管理者との間の契約の履行、またはデータの対象者の要請による契約前の措置の実施のために必要である」場合、「移転がデータの対象者のために管理者と第三国との間で締結された契約の作成又は履行のために必要である」場合など6項目を、また26条2項では「データの管理者が、プライバシー、基本権、自由の保護などに対応する権利の行使に関する十分な保護措置（adequate safeguards）を提示する」場合、さらに26条4項では、EU委員会の承認による標準契約条項による場合を、その例外としている。

したがって、EU構成国に所在する欧州本社などから、日本などの第三国に個人データを移転する際、移転先企業と個別に契約を締結するか、または企業グループ内であれば、個人データの移転に関するルールを作成し、EU域内のデータ保護機関に承認を受けるなどの例外的な方法により個人データの移転を行っている。または、個々人の同意を得て移転することも可能であるが、移転する個人データの数が少ない場合に限られる。

一方で多くの企業は、これら諸手続きの煩雑さから、そもそも個人データを、日本を含むEU域外の第三国に移転せず、EU域内の企業で完結している場合も少なくない<sup>5)</sup>。

このように、EUデータ保護指令第25条第1項の規定は、わが国企業の国際展開における「見えない障壁」となっている。わが国は、EUデータ保護指令第26条に規定された例外的措置を

---

4) 堀部政男「プライバシー・個人情報保護の国際的整合」堀部政男編著『プライバシー・個人情報保護の新課題』（商事法務、2010年）52頁。2009年4月23日に開催したブリュッセルのデータ保護会議において、欧州委員会・司法自由安全総局（European Commission Directorate-General-Justice, Freedom and Security）法務政策部（Legal Affairs and Policy）ユニットD5・データ保護（Unit D5-Data Protection）事務官（Desk Officer）ハナ・パチャコバ氏（Ms. Hana Pachackova）による「充分性認定手続（Adequacy finding procedure）」のプレゼンテーションの中で言及されたと紹介されている。

5) 消費者庁「国際移転における企業の個人データ保護措置調査 報告書」2010年、25-29頁、「(3) 日系企業の対応状況」参照。

いかに利用するかという議論を行うのではなく、欧州委員会に対して申請を行い、「保護の十分性」の認定を受けるべきである。そのためには、EUデータ保護指令が求める「十分な保護措置」の要件を充足する法制度を定立する必要がある。

## 2 EUデータ保護指令における「十分な保護措置」

わが国においては、EUデータ保護指令発効当時、公的部門を対象とした行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（以下、「行政機関個人情報保護法」という。）が存在した。同法は、その対象を「電子計算機処理を行う電子的または電磁的情報」を個人情報と定義し、手作業処理（マニュアル処理）の個人情報についてはその適用対象外となっていたこと、また公的な部門だけを対象としていたことから、EUデータ保護指令における「保護の十分性」との整合に問題があり、新たな法律の制定が急務となった。

2003年5月23日、民間部門を対象とする個人情報の保護に関する法律（以下、単に「個人情報保護法」という）が成立し、同年5月30日に一部施行された。このようにわが国は法制度の整備を進めてきたが、現在でも前述のように、わが国はEUによって、「十分なレベルの保護」を提供している国であるとは考えられていない。

その原因は、表1に示したように、EUデータ保護指令との数多くの相違にある。たとえば、EUデータ保護指令第12条において、本人が情報保有者に対して行う情報の開示・訂正・削除などを「アクセス権（right of access）」として権利構成しているが、わが国の個人情報保護法第25条では「個人情報取扱事業者の義務」として出訴可能な権利としていない点、EUデータ保護指令第8条第1項では、「人種、民族、政治的見解、宗教、思想、信条、労働組合への加盟に関する個人データの処理、もしくは健康又は性生活に関するデータ」などのセンシティブ情報の処理を原則として禁止しているが、わが国の個人情報保護法ではこのような規定がないこと、などがその原因と考えられる。

表1 EUデータ保護指令とわが国の個人情報保護法の相違

	EUデータ保護指令	日本の個人情報保護法
適用の対象	個人、法人、公的機関等	5000件を超える個人データを保有する事業者が対象であり、それ未満の事業者は法の適用から外れる
情報の種類	センシティブ情報の収集を制限	情報の質による法律上の義務の違いはない
開示請求等	出訴可能な権利（right）として構成し、法のエンフォースメントに関与できる	事業者の義務であり、出訴可能な権利として構成していない
第三国への移転	「十分なレベルの保護」でない第三国への情報の移転を制限	なし
監視機関	「完全なる独立性」の要件を具備した監視機関が官民双方を監視	主務大臣が民間を監視 行政の監視機関はない

出所）各種資料により筆者作成

### 3 監視機関

EUデータ保護指令における「十分な保護措置」の要件として最も重要なものは、「監視機関」ではないかと筆者は考える。

EUデータ保護指令第29条作業部会はこれまでに、スイス、カナダ、アルゼンチン、アメリカ合衆国セーフハーバー・スキーム、ガーンジー（Guernsey）、マン島（Isle of Man）、ジャージー（Jersey）、フェロー諸島（Faeroe Islands）について「保護の十分性」の認定を行い、また2009年12月1日に、イスラエル（Israel）およびアンドラ（Andorra）について十分性を認める意見を採択した<sup>6)</sup>。これらの国と地域に共通する要件として、民間部門のみならず公的部門の個人データ保護の状況を監視する機関が存在し、「独立性」を確立している。たとえば、イギリスの「インフォメーション・コミッショナー制度」は独立した法執行機関として300人を超えるスタッフを独自に採用し、官民双方の監視を行うとともに、国民への情報提供などを行っている。

わが国では、前述のように、2011年1月31日に公表された「政府の基本方針」、および同年6月30日に公表された「社会保障・税番号大綱」において、第三者機関の設立を規定している。この第三者機関は、「マイナンバー」の監視に限定しているものの、今後監視の対象が拡大される可能性を秘めている。現在検討されているわが国の第三者機関は「独立性」を充足しているのであろうか。

「社会保障・税番号大綱」に先立って、2011年4月28日に社会保障・税に関わる番号制度に関する実務検討会が発表した「社会保障・税番号要綱」では、「内閣総理大臣の下」に、「(国家行政組織法) 三条委員会等の設置形態を検討」とされており、官民双方の監視を行うための独立性に配慮している。このように要綱として発表された制度を検討すると、監視機関の独立性を充足しているようであり期待が持てる。

ところが、同年6月30日に公表された「社会保障・税番号大綱」では、「(国家行政組織法) 三条委員会等の設置形態を検討」という記載が削除されている。これは、国家行政組織法の八条委員会などの設置形態も検討対象とするとのことと解される。

国家行政組織法第3条は、行政組織を「府」「省」とし、その外局として「委員会」を置くことを規定している。同法第3条に基づく委員会は国家公安委員会、公正取引委員会、運輸安全委員会などがあり、「庁」と同格の独立した行政組織と見なされている。一方、同法第8条は行政機関内に審議会などを設置できると規定しており、所管省庁に従属する組織としての性格が強く、人事・予算などで所属する省庁との関係が密接であり、独立性が低いと解される。

6) 堀部政男「プライバシー・個人情報保護の国際的整合」堀部政男編著『プライバシー・個人情報保護の新課題』（商事法務、2010）49頁。

EUデータ保護指令第29条作業部会における「保護の十分性」の評価では、「完全なる独立性」を要件としていると思われることから、この第三者機関を「監視機関」として欧州委員会に申請するのであれば十分性の要件を充足しない可能性がある。

「社会保障・税番号要綱」に規定したとおり、内閣総理大臣の下に、「国家行政組織法三条委員会」の設置形態を真摯に検討すべきであろう。

#### 4 わが国のプライバシー・個人情報保護法制の重層性

わが国の個人情報保護法制は、EUとの関係のみならず、わが国における企業活動に様々な課題が散見される。それは、わが国の個人情報保護に関する法規及び企業にコンプライアンス体制の構築を求める法制度が重層的であり、企業における個人情報の利用に委縮効果をもたらしている点にある。

わが国には、2003年5月23日に成立した個人情報保護法があり、同法に基づく各省庁のガイドラインが存在する。自治体では48の都道府県と1750余の市区町村で個人情報保護条例を設けている。またプライバシーマーク制度があり、プライバシーマークの認証を希望する企業はJIS Q15001への準拠が求められる。

個人情報保護法、自治体の条例、プライバシーマークで微妙にその内容が異なり、企業はその全てに対応する必要がある。たとえば、JIS Q 15001では、センシティブ情報の取得制限を設けているが、個人情報保護法では情報の質による取扱の違いはない。またJIS Q 15001では、開示を権利として規定しているが、個人情報保護法は個人情報取扱事業者の義務として規定している。さらに、個人情報保護法およびJIS Q 15001において、「個人情報保護の基本方針」の策定を規定しているが、これは取締役会の決議事項と規定していないにもかかわらず、実質的に公表を義務付けている。一方で、2005年6月29日に成立した会社法において大会社等に求めている「内部統制の基本方針」は、取締役会での決議を義務付けているが、公開を義務付けていない。この2つの基本方針は、企業においてどのように扱ったらよいのか明確にされていない。

そのうえ、個人情報の取得時に明示した利用目的を個人情報と共に管理する必要があるが、企業はこのために多額の費用をかけて既存のデータベースを改修し、また膨大な労力をかけてその利用を制限している。

個人情報保護法は、その目的において「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」（第1条）と規定しており、権利利益の保護を図りつつも有用な個人情報の利用を促進することを目指しているにもかかわらず、このような重層的な構造の法令が利用に委縮効果をもたらしている。

これほど企業は管理上の労力と費用をかけているにもかかわらず、前述のようにEUによる

わが国のプライバシー保護に関する評価が低く、EU構成国からわが国に個人データの移転を行うことは原則として禁止されている

このように、わが国の個人情報保護法は、多くの面で課題を抱えている。これを解決するためには、現行の個人情報保護法を改正し、新たにプライバシー保護法制を定立しなければならないだろう。

## 5 情報流出事件と企業の損害

企業による情報流出事件が相次いでいる。例えば、2009年7月14日に発覚したアリコジャパン顧客情報漏えい事件は、32,359件の顧客情報が流出し、5,122件のカードの不正使用があった。また2011年4月には、ソニーが運営するプレイステーションネットワークにおける大規模な個人情報流出事件が発覚した。本件の個人情報の流出数はプレイステーションネットワークの全利用者、約7,700万人といわれている。

個人情報のみならず、企業による営業秘密流出事件も増えている。たとえば、2007年には、自動車部品メーカー大手のデンソーから、13万点に及ぶ設計図等の技術情報を、従業員である中国人技術者が持ち去った事件も起きている。

企業における情報の窃取・不正取得が目立つのは、企業が保有する様々な資産の中でも、デジタル情報が盗み取りやすく、換金性に優れ、また窃取後の利用価値が高いためと思われる。不正取得された情報が個人情報であれば、広く市民のプライバシーを侵害し、二次的な被害を引き起こす可能性がある。

情報漏えい事件は、情報の保有者である企業に対し、顧客対策費等の支出や、販売機会の逸失による売上の減少など、業績に直接的な影響を与え、また、社会的信用の毀損などによる間接的な影響も与えることとなる。

表2 近年発生した主な情報流出事件

2004年	ヤフーBB顧客情報流出事件	460万件（内部者の窃取）
2006年	防衛庁／自衛隊「秘」扱い情報流出事件	
2007年	大日本印刷個人情報流出事件	863万件（委託先社員の窃取）
2007年	デンソー技術データ流出事件	13万点の図面（内部者の窃取）
2007年	警視庁捜査情報流出事件	1万件
2009年	アリコ顧客情報漏えい事件	13万件
2009年	三菱UFJ証券顧客情報流出事件	148万件
2010年	尖閣諸島沖ビデオ映像流出、警視庁国際テロ捜査資料流出	
2011年	ソニー個人情報大量流出事件、など	

出所）各種資料により筆者作成



個人情報漏えい事件を法的な観点から幅広く考えてみる。当該情報が個人情報であれば、これを保有していた企業等は、プライバシー侵害を根拠とする本人からの訴訟リスク、個人情報保護法における安全管理義務違反による罰則リスク、委託元から預託された情報であった場合は、契約違反として損害賠償請求を受けるなどの契約リスク、情報漏えいの損失が会社法上の取締役の善管注意義務違反（内部統制システム構築義務への違反）に起因するものであれば、株主代表訴訟リスクを、それぞれ負うこととなる。

本人からの訴訟リスクの根拠は不法行為（民法第709条）である。不法行為は、「故意又は過失」、「権利侵害」、「損害の発生」、「加害行為と損害の因果関係」を要件とする。個人情報保護法は行政取締法規であるため、情報漏えいの被害を受けた本人が直接に企業を提訴することはできない。しかし、個人情報保護法によって、個人情報の収集、利用、提供、管理等の各レベルにおいて、個人情報の侵害を未然に防ぐための行為規範が設けられていることから、不法行為の要件としての違法性判断にあたって、通説である相関関係説の下、被侵害利益の要保護性が高まったという評価が可能であろう。それに伴い、企業が賠償責任を負う可能性も高まったといえるだろう。

個人情報保護法に基づく行政行為は間接罰の形を取っているため、主務大臣の勧告、命令を経ない限り、事業者が処罰を受けることはない（個人情報保護法第56条）。しかし、みちのく銀行が約131万件の顧客情報を漏えいさせた事件において、金融庁は、2005年5月20日、個人情報保護法第34条1項に基づき勧告を下した。特に金融機関の場合は銀行法上の業務停止命令に至る可能性があり、事業継続リスクに発展する可能性がある。

最もリスクが高いと考えられるのは、契約に基づき受託した情報を漏えいするケースであろう。委託元は委託先に対し、契約違反を根拠として、漏えいに起因する損害の賠償を請求することとなる。また、委託元が金融機関であるなど、主務官庁の規制が厳しく、情報漏えいが当該事業の許認可に直結する業種においては、委託元の事業継続リスクに直結することとなる。他方、漏えい事件を起こした委託先企業にとっては、膨大な損害の賠償と信用の低下により事業存続にかかわる大きなクライシスに直面する可能性がある。

株主代表訴訟リスクは、会社法第348条4項、第362条5項、および第416条2項における、大会社等の取締役の義務として、内部統制の基本方針の決定を新たに取締役の義務として規定した。この「内部統制システム」は、「会社の業務の適正を確保する」ことを目的とした統制システムである。特に個人情報保護法第20条は、「安全管理措置」を個人情報取扱事業者の義務として規定している。つまり、個人情報漏えい等の事故を未然に防止する体制の未整備は法令違反であり、その結果としての個人情報漏えいに係る損失は、取締役の善管注意義務違反に起因すると解される可能性がある。

このように情報漏えいに係る損害は、経済的な損害の大きさのみならず、法的リスクも高く、情報セキュリティは「経営上、最も重要な事項のひとつ」であるといって差し支えないので

はないだろうか。

## 6 個人情報窃盗罪の検討

わが国では、1974年には企業秘密漏示罪が検討されたが、草案の段階から賛否両論が激しく対立した。不法行為による損害賠償請求などによって保護されていることなどを鑑みると、刑法の謙抑性の観点から安易に刑法上の処罰規定を新設すべきでないとする意見、退職者に対する規定は職業選択の自由を害するおそれがあること、企業における内部告発を妨げる効果があること、などの消極論が優勢であり、結果として同条は継続検討となった。

2002年7月3日、首相直属の私的懇談会である「知的財産戦略会議」は、同年、著作権や営業秘密などの保護強化を通じた経済活性化のための行動計画である「知的財産戦略大綱」を決定した。これを受けて、経済産業省産業構造審議会知的財産政策部会不正競争防止小委員会にて、不正競争防止法の改正による営業秘密の保護に関する議論が行われ、2003年に成立した改正不正競争防止法において刑事罰としての営業秘密侵害罪が導入された。

現在、営業秘密侵害罪は、営業上又は技術上の有用性を有する情報を不正に取得する行為をその対象としているが、企業は個人情報の不正取得行為についても、営業秘密侵害罪を活用し、企業防衛上の対策を講じている。

しかし、企業が保有する顧客情報などの「個人情報」について、その不正取得行為を経済法である不正競争防止法によって刑事罰を適用することに疑問がある。わが国は、その客体である情報の価値によらず、情報窃取という行為態様に対する刑事罰の創設を検討すべきではないだろうか。

2006年1月24日、自由民主党政務調査会 e-Japan重点計画特命委員会 情報漏洩罪検討プロジェクトチームは、個人情報保護法の改正案を公表した。その中で、個人情報漏示罪を以下のように示した。

### 「第五十五条の二

個人情報取扱事業者の業務又は個人情報取扱事業者から個人データの取扱いの委託を受けた者の当該委託に係る業務に従事している者又は従事していた者が、その業務に関して知り得た個人データを自己又は第三者の不正な利益を図る目的で提供したときは、一年以下の懲役又は50万円以下の罰金に処する。

2 前項の規定の適用に当たっては、表現の自由、学問の自由、信教の自由及び政治活動の自由を不当に妨げることをないように配慮しなければならない。」

その後の民主党への政権交代により、前掲の個人情報保護法改正案は、国会で検討されるこ

とはなかったが、個人情報の不正取得行為への刑事罰導入の検討が望まれる。

## 7 むすびにかえて

現在、わが国における個人情報の利活用が萎縮しており、その結果、日本社会の中での人と人とのつながりが希薄になったといわれている。これは、個人情報保護法および関係諸法令によるところが大きい。新たなプライバシー保護法制の定立が必要ではないだろうか。

その際、EUとの間の見えない経済障壁の除去を目指す必要がある。すなわち、EUデータ保護指令第25条第1項における「十分なレベルの保護」を確保し、欧州委員会に保護の十分性評価の申請を行うべきであろう。そのためには、現在検討されている番号法における第三者機関について、「完全なる独立性」を確保することが第一歩となる。その上で、新たな情報法則を定立するとともに、地方自治体における個人情報保護条例および個人情報保護審査会、JIS Q 15001 およびプライバシーマーク制度の存続の是非についても議論を進める必要がある。

現在の個人情報保護法制は、必ずしもわが国の市民生活や企業活動において利活用と保護のバランスを実現するものになっていない。社会生活の中で必要な利活用は萎縮せずでき、一方で悪用を防ぐ罰則規定を設けるなど、個人情報の利活用と保護のバランスがとれる、新たな法制度や社会システムの設計が、わが国において急務である。

### 参考文献

- 堀部政男『現代のプライバシー』（岩波書店、1980年）。
- 堀部政男編著、高野一彦他著『インターネット社会と法 第2版』（新世社、2006年）。
- 堀部政男編著、高野一彦・鈴木正朝他著『プライバシー・個人情報保護の新課題』（商事法務、2010年）。
- 新保史生『プライバシーの権利の生成と展開』（成文堂、2000年）。
- 園部逸夫『個人情報保護法の解説』（ぎょうせい、2003年）。
- 岡村道久『個人情報保護法』（商事法務、2009年）。
- Alan F. Westin, *Privacy and Freedom*, 7 (1967).
- 佐久間修『刑法における無形的財産の保護』（成文堂、1991年）。
- 田中宏司『CSRの基礎知識』（日本規格協会、2007年）。
- 水尾順一、田中宏司『CSRマネジメント—ステークホルダーとの共生と企業の社会的責任—』（生産性出版、2004年）。
- 水尾順一『CSRで経営力を高める』（東洋経済新報社、2005年）。
- 高野一彦『情報法コンプライアンスと内部統制第2版』（ファーストプレス、2008年）。