

■S1 群（情報環境とメディア）-7 編（情報倫理・制度）**2 章 プライバシーと情報倫理**

（執筆著者：鶴原稔也）[2011年10月受領]

■概要■

プライバシーと情報倫理は密接に関係しており、本章では「プライバシー保護」、「個人情報保護」、「通信の秘密」、「情報セキュリティポリシー」、「著作権侵害」について述べている。プライバシー保護については、米国および日本における歴史的経緯について主な裁判例に沿って述べている。個人情報保護では、日本、欧州、OECDでの取り組み経緯や2003年に成立した日本の「個人情報保護法」について述べている。通信の秘密では、インターネット時代に合った解釈や新たな法律について述べている。情報セキュリティポリシーでは、コンピュータウィルスやサーバ攻撃などへの対処を体系的かつ組織的に行うために必要な考え方や手順について述べている。著作権侵害では、デジタル技術やインターネットなどの発展に伴い増大している著作権にかかわる紛争について最近の裁判事例を含めて述べている。

■S1 群 - 7 編 - 2 章

2-1 プライバシー保護

(執筆者：鶴原稔也) [2011年10月受領]

プライバシー及びその権利(以下、「プライバシー権」という)は、現在では高度に発達した文明社会における極めて成熟した高級な人格権の一つとして認知されているが、その歴史はそれほど古いものではない^{*1}。ただ、プライバシー権の権利範囲は明確でなく、時代とともに変遷し、また論ずる人によっても定義が異なっていることが多い。そのため、日本の個人情報保護法制定時にもプライバシー権との関係が議論されたが、プライバシー権に確立された定義がない^{*2}、との理由により個人情報保護法はプライバシー権とは独立したものとして制定された。

現在のプライバシー権は、次の三つの要素から成っているとされている^{*3}。

- ① 一人にしておいてもらうという「侵入からの自由」
- ② 自己情報のコントロール
- ③ 監視からの自由(尾行、観察、盗聴からの自由)

近年、プライバシー権侵害が問題になることが多いのは、コンピュータやインターネットの発達が密接に関係している。コンピュータやインターネットを使用することにより、これまで成し得なかった大量情報の集中と処理が可能になり、しかも多くの場合本人に知られずに当人の個人的な情報を収集することが可能となったことが、プライバシー侵害を発生させる遠因となっている。

人は社会的な生物であり、一人で生きていくことはできないため完全にプライバシーを守って生活することはできない。このため、他の利益を得るためにプライバシーをどれだけ放棄するか、というジレンマが発生する。

歴史的には、米国において1890年にSamuel WarrenとLouis Brandeisが「プライバシーの権利」に関する論文を発表したのがプライバシーを独立した権利であると主張した最初といわれている。この論文で、WarrenとBrandeisは、「プライバシー権」は「ひとりで居させてもらう権利」だと主張した。19世紀末の米国は、読者の好奇心に訴えるためにセンセーショナルリズムが横行し始めた時期であった。ハリウッドスターなどの有名人がイエロージャーナリズムに無断で私生活を写真に撮られる事例が多発していた。プライバシー権は、イエロージャーナリズムに対して防御する目的で「ひとりで居させてもらう権利」として発表された。

1902年にはロバーソン事件米国最高裁判決が出された。これは、製粉会社が自社の宣伝用に大量配布した印刷物に自分の顔が無断掲載されたので、周囲から冷やかかしや嘲りを受けて身体と精神とに苦痛と被害を受けた女性が差止と損害賠償を求めて製粉会社を提訴した事件であった。最高裁は、プライバシーの権利性を否定して請求を棄却した。この最高裁判決には批判が多く集まり、翌年の1903年にはロバーソン事件最高裁判決に反発した世論を背景に、ニューヨーク州議会がプライバシーの権利を認める州法を制定した。

*1 青柳武彦, “情報化時代のプライバシー研究「個の尊厳」と「公共性」の調和に向けて,” NTT 出版, pp.7, 2008.

*2 個人情報保護法制定時の起草者国会答弁.

*3 Sara Baase (日本情報倫理協会(JANL)(訳)), “IT社会の法と倫理(第2版),”ピアソン・エデュケーション, pp.34, 2007.

1905年には、パイプジック事件ジョージア州米国最高裁が、自己の肖像写真を無断で新聞広告に使用した保険会社を提訴した事件で、幸福追求権を根拠にプライバシー侵害の権利性を認める判決を出した。

1931年には、メルビン事件カリフォルニア州米国最高裁が、無断で原告の実名入り映画を上映した結果、売春婦であり殺人事件被告人として無罪判決を受けた原告の過去が暴露され、更正後に結婚して平穏に過ごしていた新生活が破綻に至った事件において、「プライバシーはひとりで居させてもらう権利」であるとし、原告勝訴の判決を出した。

1965年には、米国の連邦政府がラッグルズ報告に基づいて「ナショナル・データセンター構想」を発表した。これは、連邦内の機関が保有する個人情報のコンピュータによる集中管理を行うという構想であった。しかしながら、この構想は米国国民の反発で頓挫した。1967年には、アラン・ウェスティンコロロンビア大学教授が著書「プライバシーと自由」を発表した。

1971年には、アーサー・ミラーが「プライバシーへの攻撃」を発表した。これは、Warrenと Brandeis の「ひとりで居させてもらう権利」を進め、プライバシーの権利を「自己に関する情報の流通をコントロールできる権利」(自己情報コントロール権)として把握しようとするものであった。

このようにプライバシー権として独立した権利として認める流れはあるが、これに対しての批判もある。Warrenと Brandeisの見解に異を唱えたのがJudth Jarvis Thomsonである。Thomsonは、プライバシー権は独立して存在するものでなく、必ず他の権利と一緒にあり、「私は、プライバシー権なるものが侵害されているような場合、何がしかの権利が実際に侵害されているかどうかを問うまでもなく、当該行為が他の権利を侵害しているかどうかを問うた方が、回答発見の手段(Heuristic Device)としては有用であると言わんとしているのだ」*4。

一方、日本におけるプライバシー権保護に関する歴史は以下の通りである。

1964年の大阪証券労組保安阻止デモ事件控訴審判決において、日本の判例上初めて「プライバシー権」が登場したといわれている。

更に、同じ年に、三島由紀夫著の「宴のあと」事件判決が東京地方裁判所において出された。これは、三島由紀夫が、雑誌「中央公論」の昭和35年1月号から同年10月号に連載執筆した「宴のあと」において、主要人物である「野口雄賢」が原告「有田八郎」を、「福沢かづ」が「畔上輝井」をさしていることは明らかであり、その効果は実名を挙げた場合と異ならないとして、有田八郎が提訴したものである。東京地方裁判所の判断は、プライバシー権は、「私生活をみだりに公開されないという法的保障ないし権利」として、以下の三つの条件が満たす場合、保護されるとした。

(イ) 私生活上の事実または私生活上の事実らしく受け取られるおそれのあることがらであること。

(ロ) 一般人の感受性を基準にして当該私人の立場に立った場合、公開を欲しないであろうと認められることがらであること、換言すれば一般人の感覚を基準として公開されることによって心理的な負担不安を覚えるであろうと認められることがらであること。

*4 Sara Baase (日本情報倫理協会(JANL)(訳))、「IT社会の法と倫理(第2版)」,ピアソン・エデュケーション, pp.76-77, 2007.

(ハ) 一般の人々に未だ知られていないことがらであること。

上記の三つの条件はその後プライバシー権保護の条件とされている。

1970年には、政府が電算化推進の一環として各省庁に統一的な事務処理用個人コードを設定する制度、いわゆる「国民総背番号制」導入を閣議決定した。しかしながら、世論の反発により政府は導入を中止した。

1987年には、ノンフィクション「逆転」事件判決が東京地方裁判所において出された*5。本判決において、東京地方裁判所は以下の三つの守るべき項目を示した。

- ① 他人がみだりに個人の私的事柄についての情報を取得することを許さず、
- ② 他人が自己の知っている個人の私的事柄をみだりに第三者へ公表したり、利用することを許さず、
- ③ 人格的自律ないし私生活上の平穩を維持するという利益（プライバシーの権利）は十分尊重されるべきであること。

本件については、1994年2月8日に最高裁判所は上告を棄却し原告勝訴で確定している。

*5 東京地裁判昭和62年11月20日。

■S1 群 - 7 編 - 2 章

2-2 個人情報保護

(執筆者：鶴原稔也) [2011年10月受領]

「個人情報」とは個人にかかわる情報のことであり、「プライバシーの権利」と密接に関係するが同一ではない。

2003年5月23日に国会で可決成立し、5月30日に交付された「個人情報の保護に関する法律」*6では、個人情報の定義を次のように定めている。

『この法律において「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。（第2条（定義））』

1970年代の欧州においては、各国が独自に個人情報保護に関する法律を定めていたが、グローバル化の進展に伴って各国毎の規制が円滑な経済活動の支障となってきた。そこで、経済協力開発機構（OECD）において統一的なガイドラインの策定に向けての議論が行われ、その結果、1980年にOECDは「プライバシー保護と個人データの流通についてのガイドラインに関する理事会勧告」（いわゆる『OECD プライバシーガイドライン』）を採択した。本ガイドラインにおいてOECD 8原則が規定されており、これらには法的拘束力はないが、その後の日本を初め加盟各国の個人情報保護法制定に大きな役割を果たした。

OECD 8原則*7の内容は次の通りである。

- ① 目的明確化の原則…収集目的を明確にし、データ利用は収集目的に合致するべき。
- ② 利用制限の原則…データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用してはならない。
- ③ 収集制限の原則…適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき。
- ④ データ内容の原則…利用目的に沿ったもので、かつ、正確、完全、最新であるべき。
- ⑤ 安全保護の原則…合理的な安全保障措置により、紛失・破壊・使用・修正・開示などから保護するべき。
- ⑥ 公開の原則…データ収集の実施方針などを公開し、データの存在、利用目的、管理者などを明示するべき。
- ⑦ 個人参加の原則…自己に関するデータの所在及び内容を確認させ、または異議申し立てを保証すべき。
- ⑧ 責任の原則…管理者は諸原則実施の責任を有する。

上記のOECD 8原則を受けて各国で個人情報保護への取り組みがなされたが、各国ごとの取り組みであり、また全体を包括するようなものではなかった。

このようななか、欧州では個人情報保護への取り組みが積極的に行われ、1995年10月24日に、「個人データの取扱い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欧州議会及び理事会の指令（EU データ保護指令）」が出された。これは、個人データ（情報）の取り

*6 平成15年法律第57号。

*7 消費者庁ホームページ「個人情報の保護」, <http://www.caa.go.jp/seikatsu/kojin/kaisetsu/>

扱いに関する基本的権利と自由を保護するために制定されたものである。

この EU データ保護指令では「個人情報」ではなく、「個人データ」という用語を用いており、その定義は次のようになっている。『個人データとは、識別された又は識別され得る自然人（以下「データ主体」という。）に関するすべての情報をいう。識別され得る個人とは、特に個人識別番号、又は肉体的、生理的、精神的、経済的、文化的並びに社会的アイデンティティに特有な一つの又は二つ以上の要素を参照することによって、直接的又は間接的に識別され得るものをいう。（第 2 条、定義）』

EU データ保護指令の対象は EU 構成国である 27 개국であるが、① EU 構成各国に対して、3 年以内に指令に適合するように個人データ保護のための法制化を行うこと、② EU 域外の第三国への個人データの移転はその第三国が十分なレベルの個人データ保護措置を行っている国に限定し、保護措置が十分であると認められない場合には、その第三国と交渉を開始しなければならない、と第三国への情報の移転に関して規定し、EU 以外の国へ大きな影響を与えた^{*8,*9}。

上記の EU データ保護指令により自国企業が EU 企業や政府などと自由な情報の流通が阻害されるのではないかと危惧した米国政府は EU と協議を開始し、包括法がない米国では個別に認定する「セーフハーバー方式」を採用することで合意が成立し、EU と米国間の情報の流通が円滑に行えるようになった。

また、日本でも高度情報通信社会の進展に伴い個人情報保護をはかるべきであるとの認識が広がっていた状況に加え、上記の EU データ保護指令への対応が求められた。1997 年には、「経済構造の変革と創造のための行動計画」が閣議決定され、電子商取引の普及に向けて必要な法整備を行うこととした。1997 年に通商産業省（現経済産業省）が「個人情報保護に関するガイドライン」を改定し、さらに、翌年には「プライバシーマーク制度」が発足した。

1999 年に成立した「住民基本台帳法」の国会審議において個人情報保護法が日本ではない

*8 消費者庁ホームページ「諸外国等における個人情報保護制度の運用実態に関する検討委員会・報告書（平成 19 年 1 月）」、<http://www.caa.go.jp/seikatsu/shingikai/kojin/20th/20070305kojin2-1.pdf>

*9 25 条（原則）

1. 構成国は、取り扱われている又は移転後に取扱いが予定されている個人データの第三国への移転は、この指令に従って採択された国内規定の遵守を損なうことなく、当該第三国が十分なレベルの保護措置を確保している場合に限って、行うことができることを定めなければならない。
2. 第三国によって保障される保護のレベルの十分性は、一つのデータ移転作業又は一連のデータ移転作業に関するあらゆる状況にかんがみて、評価されなければならない。特に、データの性質、予定されている取扱作業の目的及び期間、発信国及び最終の目的国、当該第三国において有効である一般的及び分野別の法規範、並びに当該第三国において遵守されている専門的規範及び安全保護対策措置が考慮されなければならない。
3. 構成国及び委員会は、第三国が 2 項の規定の意味における十分なレベルの保護を保障していないと考えられる事例について、相互に情報提供しなければならない。
4. 構成国は、31 条 2 項に規定する手続に基づいて委員会が、第三国が本条 2 項の規定の意味における十分なレベルの保護を保障していないと認定した場合には、当該第三国への同一タイプのデータの移転を阻止するために必要な措置を講じなければならない。
5. 委員会は、適切な時期に、4 項に基づく認定によってもたらされる状況を改善することを目的として交渉を開始しなければならない。
6. 委員会は、31 条 2 項に規定する手続に基づいて、第三国が私生活、個人の基本的な自由及び権利を保護するための当該第三国の国内法、又は特に本条 5 項に規定された交渉の結果に基づいて締結した国際公約を理由として、2 項の規定の意味における十分なレベルの保護を保障していると認定することができる。

ことへの懸念が強まり、当時の小渕総理大臣が、『民間部門をも対象とした個人情報保護のあり方について総合的に検討した上で、法整備を含めたシステムを速やかに整えていきたい。』と述べ、民間部門も含めた個人情報保護法制を整備することを明言した。

個人情報保護法の法制化はその後国会に関連法案が提出され審議されたが、マスメディアなどの反対があり難航した。2003年に関連法案と共に「個人情報保護関係5法」が国会で可決成立し、2005年4月1日に完全施行された。個人情報保護法制の体系イメージを図2・1に示す^{*10}。

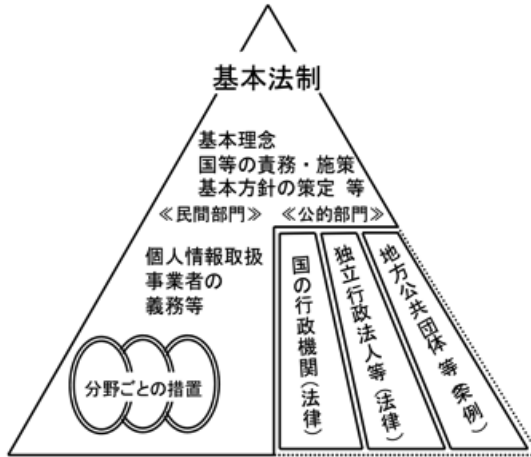


図2・1 個人情報保護法制の体系イメージ（出典：消費者庁ホームページ^{*10}）

個人情報保護関係5法とは、次の五つの法律をいう。

- ① 個人情報保護法（基本法）
- ② 行政機関個人情報保護法
- ③ 独立行政法人等個人情報保護法
- ④ 情報公開・個人情報保護審査会設置法
- ⑤ 整備法

個人情報保護を図るための法律を制定する際に、公的部門と民間部門を一つの法律で扱う場合（これを「オムニバス方式」という）、別の法律で扱う場合（これを「セグメント方式」という）に大別される。EUは前者、米国は後者の体系を採用しているが、日本はこれらの折衷方式であり、基本法的部分に関してはオムニバス方式、一般法的部分に関してはセグメント方式となっている。更に、日本では個人情報保護を図るための統一的な組織は存在せず、各省庁が管轄する分野に関するガイドラインを作成して各分野ごとに個人情報の保護を図る仕組みとなっている。この方式では各分野の特徴に沿った保護が図れるというメリットがある反面、それぞれのガイドラインに統一性がなく、場合によっては保護の程度に差があり、混乱が生じるというデメリットもある。各省庁のガイドラインは消費者庁のホームペー

*10 消費者庁ホームページ、<http://www.caa.go.jp/seikatsu/kojin/kaisetsu/pdfs/taikei.pdf>

ジ^{*11}に一覧が掲載されているので参照されたい。

個人情報保護法で定めている個人情報取扱事業者の義務としては、次の事項が規定されている。

- ① 利用目的の特定，利用目的による制限（個人情報）。
 - ・利用目的をできる限り特定しなければならない（第15条）。
 - ・特定された利用目的の達成に必要な範囲を超えて取り扱ってはならない（第16条）。
- ② 適正な取得，取得に際しての利用目的の通知等（個人情報）。
 - ・偽りその他不正な手段により取得してはならない（第17条）。
 - ・取得した場合は，あらかじめその利用目的を公表している場合を除き，速やかに，その取得目的を本人に通知し，又は公表しなければならない（第18条）。
- ③ データ内容の正確性の確保（個人データ）。
 - ・個人データを正確かつ最新の内容に保つように努めなければならない（第19条）。
- ④ 安全管理処置，従業者・委託先の監督（個人データ）。
 - ・取り扱う個人データの漏洩，滅失又はき損の防止その他の個人データの安全管理のために必要な適切な措置を講じなければならない（第20条）。
 - ・従業者・委託先に対して必要な監督を行わなければならない（第21条，22条）。
- ⑤ 第三者提供の制限（個人データ）。
 - ・本人の同意を得ないで，個人データを第三者に提供してはならない（第23条）。
- ⑥ 公表等，開示，訂正等，利用停止等（保有個人データ）。
 - ・利用目的等を本人の知り得る状態に置かなければならない（第24条）。
 - ・本人の求めに応じて保有個人データを開示・訂正・利用停止等を行わなければならない（第25，26，27条）。
- ⑦ 苦情の処理（個人情報全般）。
 - ・苦情の適切かつ迅速な処理に努めなければならない（第31条）。

個人情報保護法において個人情報取扱事業者の適用が除外されているのは、次のとおりである（第50条）。

- 一 放送機関，新聞社，通信社その他の報道機関（報道を業として行う個人を含む）…報道の用に供する目的。
- 二 著述を業として行う者…著述の用に供する目的。
- 三 大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者…学術研究の用に供する目的。
- 四 宗教団体…宗教活動（これに付随する活動を含む）の用に供する目的。
- 五 政治団体…政治活動（これに付随する活動を含む）の用に供する目的。

*11 消費者庁ホームページ，<http://www.caa.go.jp/seikatsu/kojin/gaidorainkentou.html>

■S1 群 - 7 編 - 2 章

2-3 通信の秘密

(執筆者：鶴原稔也) [2011年10月受領]

通信の秘密の保障は、日本国憲法第 21 条第 2 項後段^{*12} において明文化されている。

その趣旨は、個人の私生活の自由を保護し、個人生活の安寧を保障する（プライバシーの保護）とともに、通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段であることから、思想表現の自由の保障を実効あらしめ、自由闊達な通信がなされることを保障することにある。通信の秘密とは、通信の内容にとどまらず、通信当事者の住所、氏名、発信場所など通信の構成要素や通信回数などの通信の存在の事実の有無を含む概念であり、個人にかかわる通信の秘密は、個人識別情報としての当該通信当事者の個人情報に包摂される。また、「通信の秘密を侵す」とは、通信当事者以外の第三者が積極的意思をもって「知得」しようとするもののほか、第三者にとどまっている秘密をその者が「漏えい」（他人の知り得る状態にすること）すること、及び、「窃用」（本人の意思に反して自己または他人の利益のために用いること）することを含むと解されている。通信に関して知り得た他人の秘密とは、「通信の秘密」のほか、通信当事者の人相、言葉の訛やプッシュホンに記憶された相手番号など、直接の通信の構成要素とはいえないが、それを推知させ得るものを意味する^{*13}。これを担保するために、電気通信分野では、電気通信事業法（第 4 条）、有線電気通信法（第 9 条）、電波法（第 59 条）において通信の秘密を保護する規定が置かれている。また、関連する法律として、「不正アクセス行為の禁止等に関する法律」（いわゆる「不正アクセス禁止法」）があり、不正アクセス行為を禁止している。

組織的な犯罪への対応として、通信の秘密を害することなく電気通信の傍受を行うために、「犯罪捜査のための通信傍受に関する法律」（いわゆる「通信傍受法」）が制定されている。そのなかでは、検察官らは裁判官の発する傍受令状により、電話番号その他発信元または発信先を識別するための番号または符号によって特定された通信の手段を用いて行われた犯罪関連通信の傍受をすることができるとされている。

インターネットへの接続を提供するインターネットサービスプロバイダ（Internet Service Provider：ISP）は、日本では電気通信事業者の一つとして位置づけられており、事業者および従業員は通信の秘密を守ることが義務づけられている。インターネットを用いた著作権侵害やプライバシーの権利侵害などが深刻になるに従い、侵害を行っていると思われる者を特定するために ISP が所有している情報（氏名や通信記録など）の開示請求がなされる例が多くなった。一方、通信の秘密との関係で ISP は裁判所の令状がない限り情報が出せず社会的問題となった。これを解決するために、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（いわゆる「プロバイダ責任制限法」）が制定され、一定の条件の元に情報の流通により他人の権利が侵害されたときに、プロバイダなどの特定電気通信事業者が送信を停止したことによって生じた損害賠償の責任はないとしている。

*12 第二十一条 集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。

2 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

*13 電気通信分野における個人情報保護法制の在り方に関する研究会報告書（2000年12月15日）、http://warp.ndl.go.jp/info:ndljp/pid/283520/www.soumu.go.jp/joho_tsusin/pressrelease/japanese/denki/001215j603.html#s01

■S1 群 - 7 編 - 2 章

2-4 情報セキュリティポリシー

(執筆者：鶴原稔也) [2011年10月受領]

現在の私たちの生活はコンピュータ、インターネット、携帯電話などの ICT (Information and Communication Technology; 情報通信技術) が必要不可欠となっている。一方、コンピュータウィルスやサーバ攻撃などの情報セキュリティ上の脅威も多く、また会社内の社員などによる情報漏えいも数多く発生している。

このような情報セキュリティ上の問題に対する対策は会社や大学などの個々の部門が個別に対処するのではなく、会社などのトップが基本的な方針を策定し、それに従って対処する必要がある。このような基本方針などを「情報セキュリティポリシー」という。情報セキュリティポリシーは、一般的に「基本方針」、「対策基準」、「実施手順」から構成される。

基本方針は、会社などの経営層が情報セキュリティに関する考え方や方針を記載したものであり、情報セキュリティ対策へ取り組む姿勢を明らかにするために社外に公開するのが良いとされている。

対策基準は、基本方針を受けて組織的に情報セキュリティ対策を行うために実際に守るべき事項、適用範囲および対象者などが具体的に記載されている。

実施手順は、対策基準を実施する際にどのように実施するかを記載したものであり、マニュアル的なもの、ガイドライン的なものである。

情報セキュリティ対策は、上記の「基本方針」、「対策基準」、「実施手順」を制定すれば終わりではなく、情報セキュリティ上の脅威は日々新しいものが出てきており、常に見直しが必要である。一般的に PDCA サイクルといわれている、「計画 (Plan)」、「実行 (Do)」、「評価 (Check)」、「改善 (Action)」を継続的に実行する必要がある。

情報セキュリティポリシーに関する基準としては、情報セキュリティ政策会議が 2010 年 5 月 11 日に発表した「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針 (第 3 版)*¹⁴」および「政府機関の情報セキュリティ対策のための統一基準 (第 4 版) (平成 21 年度修正)*¹⁵」に我が国における情報セキュリティ対策の基本方針が記述されている。上記指針に沿い、「政府機関の情報セキュリティ対策のための統一管理基準 (案) 及び「政府機関の情報セキュリティ対策のための統一技術基準 (案) が 2011 年 1 月 21 日期限で意見募集*¹⁶ され、検討されている。

電子情報通信学会、情報処理学会 および電気学会は、2003 年 1 月 29 日に日本政府 (内閣官房「高度情報通信ネットワーク社会推進戦略本部」) に対して共同で「高等教育機関におけるネットワーク運用ガイドライン」を提言した*¹⁷。

「電子情報通信学会ネットワーク運用ガイドライン検討ワーキンググループ」と「国立情報学研究所ネットワーク運営・連携本部」および「国立大学法人等における情報セキュリティポリシー策定作業部会」とが共同検討した「高等教育機関の情報セキュリティ対策のた

*¹⁴ http://www.nisc.go.jp/active/general/pdf/K303-101-1_draft.pdf

*¹⁵ <http://www.nisc.go.jp/active/general/pdf/K303-091.pdf>

*¹⁶ <http://www.nisc.go.jp/active/general/kijun5.html>

*¹⁷ <http://www.ieice.org/jpn/teigen/nwgl.html>

めのサンプル規程集」を2007年10月31日に公開している*¹⁸。

*¹⁸ <http://www.nii.ac.jp/csi/sp/doc/sp-sample-fy2007.pdf>

■S1 群 - 7 編 - 2 章

2-5 著作権侵害

(執筆者：鶴原稔也) [2011年10月受領]

著作権法は当初小説、音楽、絵画などの文学作品を保護することから始まった。その後、著作権法は設計図、コンピュータプログラム、データベースなどの産業分野にその守備範囲を拡大している。

古くはオリジナル作品の複製は印刷業者などに限定されており、著作権者は印刷業者などを管理すれば自らの利益を守ることができた。近年では、デジタル技術の進展によりオリジナルの品質を損なうことなく、また個人が安価に複製(コピー)を行うことが可能になり、著作権者が自らの著作権を管理することが難しくなっている。更に、インターネットの普及により、コピー品が瞬時に全世界に拡散するようになり、著作権侵害が非常に大きな問題となっている。

このような著作権侵害に対応するために、著作権法にコンピュータプログラムの保護^{*19}、データベースの保護^{*20}、技術的保護手段の回避^{*21}、自動公衆送信権^{*22}の創設などの対応が

^{*19} 第二条(定義) この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

十の二 プログラム…電子計算機を機能させて一の結果を得ることができるようにこれに対する指令を組み合わせたものとして表現したものをいう。

第十条(著作物の例示) この法律にいう著作物を例示すると、おおむね次のとおりである。

九 プログラムの著作物

^{*20} 第二条(定義) この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

十の三 データベース…論文、数値、図形その他の情報の集合体であって、それらの情報を電子計算機を用いて検索することができるように体系的に構成したものをいう。

第十二条の二(データベースの著作物) データベースでその情報の選択又は体系的な構成によって創作性を有するものは、著作物として保護する。

^{*21} 第二条(定義) この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

二十 技術的保護手段…電子的方法、磁気的方法その他の人の知覚によって認識することができない方法(次号において「電磁的方法」という。)により、第十七条第一項に規定する著作人格権若しくは著作権又は第八十九条第一項に規定する実演家人格権若しくは同条第六項に規定する著作隣接権(以下この号において「著作権等」という。)を侵害する行為の防止又は抑止(著作権等を侵害する行為の結果に著しい障害を生じさせることによる当該行為の抑止をいう。第三十条第一項第二号において同じ。)をする手段(著作権等を有する者の意思に基づくことなく用いられているものを除く。)であつて、著作物、実演、レコード、放送又は有線放送(次号において「著作物等」という。)の利用(著作者又は実演家の同意を得ないで行ったとしたならば著作人格権又は実演家人格権の侵害となるべき行為を含む。)に際しこれに用いられる機器が特定の反応をする信号を著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録し、又は送信する方式によるものをいう。

^{*22} 第二条(定義) この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

九の四 自動公衆送信…公衆送信のうち、公衆からの求めに応じ自動的に行うもの(放送又は有線放送に該当するものを除く。)をいう。

九の五 送信可能化 次のいずれかに掲げる行為により自動公衆送信し得るようにすることをいう。

イ 公衆の用に供されている電気通信回線に接続している自動公衆送信装置(公衆の用に供する電気通信回線に接続することにより、その記録媒体のうち自動公衆送信の用に供する部分(以下この号及び第四十七条の五第一項第一号において「公衆送信用記録媒体」という。)に記録され、又は当該装置に入力される情報を自動公衆送信する機能を有する装置をいう。以下同じ。)の公衆送信用記録媒体に情報を記録し、情報が記録された記録媒体を当該自動公衆送信装置の公衆送信用記録媒体として加え、若

なされてきた。

技術的保護手段とは、例えばCD、MD、DATなどに用いられているSCMS (Serial Copy Management System) や、DVDに用いられているCGMS (Copy Generation Management System) のように著作権法で保護されている著作物の複製を制限する技術をいう。これらの技術的保護手段を回避することは不可能でなく、コピーガードキャンセラなどのような回避専用機器が市販されており、これらを放置することは著作権などの保護が図れないこととなる。このため、技術的保護手段を回避する複製は私的複製であっても著作権侵害に当たることとした^{*23}。

紙に印刷されたものが大部分であった時代には、例えばコピー機での複製をコントロールすることにより著作権保護が図れてきた。しかしながら、現在ではアナログからデジタルへ変化し、紙ベースから電子情報へ変化している。このため、著作権保護もこのような時代の変化に対応したものにする必要がある。特に、最近ではインターネットの普及によりデジタル情報が瞬時に、かつ全世界に拡散できるようになったため、インターネットを通じて一般の人がアクセスできるサーバなどに情報を記録・入力する行為を「自動公衆送信権」や「送信化可能権」として著作権の権利範囲に含めるようにした。

新しい技術の開発は一般の人の利便性を高める反面、著作権者の利益を損ねる面も併せてもっており、常にこられるバランスを図る必要がある。インターネットやデジタル技術の発達に伴う著作権に関する紛争も増大している。例えば、ファイル交換サービス提供者が自動公衆送信権・送信可能化権侵害を問われた「ファイルログ事件^{*24}」、Winnyというファイル共有ソフトウェアを用いて映画をインターネットでダウンロード可能とした行為が公衆送信権侵害とされたWinnyファイル交換事件^{*25}、「まねきTV」という名称で放送番組を利用者からの求めに応じて自動的に送信する機能を有する機器を用いてサービスを提供していた業者が著作権法違反に問われた「まねきTV事件^{*26}」、日本のテレビ番組を録画しインターネットを通じて海外に転送できる機器「ロクラクⅡ」を製造し、サービスの加入者に販売・貸与し、海外にいる加入者が子機で録画を指示すると、日本にある親機で録画された番組が転送

しくは情報が記録された記録媒体を当該自動公衆送信装置の公衆送信用記録媒体に変換し、又は当該自動公衆送信装置に情報を入力すること。

ロ その公衆送信用記録媒体に情報が記録され、又は当該自動公衆送信装置に情報が入力されている自動公衆送信装置について、公衆の用に供されている電気通信回線への接続（配線、自動公衆送信装置の始動、送受信プログラムの起動その他の一連の行為により行われる場合には、当該一連の行為のうち最後のものをいう。）を行うこと。

^{*23} 第30条（私的使用のための複製） 著作権の目的となっている著作物（以下この款において単に「著作物」という。）は、個人的に又は家庭内その他これに準ずる限られた範囲内において使用すること（以下「私的使用」という。）を目的とするときは、次に掲げる場合を除き、その使用する者が複製することができる。

二 技術的保護手段の回避（技術的保護手段に用いられている信号の除去又は改変（記録又は送信の方式の変換に伴う技術的な制約による除去又は改変を除く。）を行うことにより、当該技術的保護手段によって防止される行為を可能とし、又は当該技術的保護手段によって抑止される行為の結果に障害を生じないようにすることをいう。第二百十条の二第一号及び第二号において同じ。）により可能となり、又はその結果に障害が生じなくなった複製を、その事実を知りながら行う場合。

^{*24} 東京地裁判決平成14年4月11日判例時報1780号25頁、東京地裁判決平成15年1月29日判例時報1810号29頁。

^{*25} 京都地裁判決平成16年11月30日判例時報1879号153頁。

^{*26} 最高裁平成21(受)653平成23年1月20日判決。

されるようにした業者が著作権法違反に問われた「ロクラクⅡ事件^{*27}」など多くの紛争が生じている。

これら著作権に関する紛争は、そもそも現在の著作権が絵画や音楽など芸術作品を対象とした時代に作られたものであり、デジタル技術やインターネットなどの現代の技術開発成果を活用する枠組みに合わなくなっており根本的に著作権法を見直すべきであるとの意見も出てきている^{*28}。

^{*27} 最高裁 平成 21(受)788 平成 23 年 1 月 20 日判決。

^{*28} 名和小太郎, “著作権 2.0 ―ウェブ時代の文化発展をめざして,” NTT 出版, 2010.