わが国の現行情報法制の課題と提言

Current problems and challenges relating to information law in Japan

関西大学　社会安全学部
髙　野　一　彦
Kansai University, Faculty of Safety Science
Kazuhiko TAKANO

SUMMARY

Japan is unappreciated as a nation to provide adequate level of privacy protection by EU, despite having put in a lot of time and effort on the protection of Personal Information. Japan has to establish a new law on privacy protection, which is praised by the international community. They are important step toward not only contributing to a decrease in leaking of personal information as social disasters, but also spurt in corporate activity and resolving domestic problems. And also, Japan shoulders the important responsibility as CSR major advanced country. In this paper, I'll suggest a framework of new privacy protection law in Japan, after carefully cleaning up problems that already exist.

Key words

Privacy, Personal Information, Trade Secret, Information Law, EU Directive

1．問題の所在

近年，グローバルに事業活動を展開するわが国の企業は，「個人情報」にかかる法や規格へのコンプライアンス活動に多くの費用と労力を費やしている．

第一は国内法規への対応である．わが国には，2003（平成 15）年 5 月 23 日に成立した個人情報の保護に関する法律（以下「個人情報保護法」という．）があり，同法に基づく各省庁のガイドラインが存在する．地方自治体では 48 の都道府県と，1,750 の指定都市を含む市町村及び特別区（2010 年 4 月 1 日現在の自治体数，指定都市の行政区は含まず）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 Q 15001 への準拠が求められる．個人情報保護法，地方自治体の条例，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．また本人から個人情報を取得する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，膨大な労力をかけてその利用を制限している．

第二は海外の法規への対応である．特にEU構成国において事業を展開し，情報の移転を行う場合は，EUデータ保護指令に基づく，「十分なレベルの保護（adequate level of protection）」でない第三国としての対応が必要である．

第三は情報流出事件への対応である．わが国においては個人情報の不正取得者への刑事罰の適用には厳しい要件が必要であり，万が一情報流出事件が起こった場合に備え，その要件を具備するように管理を行うことは企業防衛上の重要な取組みである．

このようにわが国の多くの企業は，個人情報保護への対応に多大な時間と労力を費やし，真摯に対応を行っている．筆者が2010（平成22）年5月に，社会から優良企業との評価を受けている大手企業21社を対象に実施した調査では，2000年からの10年間で，平均従業員数は4,276人から4,097人と微減であったが，コンプライアンス部門の平均社員数は5.2人から25.3人と4.8倍に増加した[1]．これらの多くの企業は，個人情報保護と内部統制への対応のために人員を増やしている．わが国の企業が，いかに真摯に個人情報保護に取組んでいるかが伺い知れよう．

ところがEUによるわが国の個人データの保護に関する評価は高くない．2009年4月23日，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.」[2]と述べたと紹介されている．

わが国の企業は，これほどの努力をしているにも関わらず，EUから十分性の評価を得られず，情報の流通に制限がかかっていることに企業の不満が募っている．「日本企業は真摯に対応を行っているにもかかわらず，EUによる評価がここまで低いということは，そもそもわが国の政策が間違っていたのではないか」[3]という感想を持っている者もいる．

本稿では誌面の制限もあることから，企業の情報管理に関して，特にEUとの関係，および情報の不正取得者への刑事罰の2つにテーマに絞って，わが国企業の置かれている状況を整理し，その問題を抽出し，新たな情報法制の提言を行いたい．

2．個人データ移転に関するEUとの関係

2.1　EUデータ保護指令

現在，EU域内において事業を行う日本企業は，個人データの移転に規制がかけられている．これは，EUにおいて，1995年10月24日に採択され，1998年10月24日に発効した「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」[4]（以下「EUデータ保護指令」という.）が，個人データの国際移転に関する規制を設けているためである．

EUデータ保護指令は，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，個人データの処理（自動処理および一部のマニュアル処理）に対して適用される．EC条約189条によると，指令（Directive）は，規則（Regulation）のように直接適用するものではないが，全加盟国が指令に基づき国内法として立法義務を有する[5]．従って，EUデータ保護指令は，EU加盟国27か国および欧州経済領域（European Economic Area, EEA）構成国であるノルウェイ，リヒテンシュタイン，アイスランドに対して，同指令に従った国内法の整備を求めている．

個人データの国際移転に関する規制は，EUデータ保護指令25条1項に規定されている．第25条第1項は，「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．」[6] としている．EU 域外諸国においても同じ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．

EU データ保護指令 25 条 1 項に規定された「十分性」の認定は，第三国の代表による公式な要請が欧州委員会に提出された場合，EU データ保護指令第 29 条作業部会（Article 29 Working Party）が評価を行い，欧州委員会が最終判断を行う [7]．

2.2　日本企業の対応

日本は，EU データ保護指令第 29 条作業部会による，「十分性」の認定手続きを申請していないが，欧州委員会関係者からは前述のように，日本の個人データの保護レベルの「十分性」を評価されていない．現在，EU 構成国に所在する企業が，日本に個人データを移転する場合は，EU データ保護指令に設けられた，例外的措置を利用することになる．

例外的措置は，EU データ保護指令 26 条 1 項，2 項および 4 項に設けられている．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，又はデータの対象者の要請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．

したがって日系企業は，EU 構成国所在の企業から，日本を含む EU 域外の第三国に所在する企業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方法により，個人データの国際移転を行っている．移転する個人データの人数が限られている場合は，個々人の同意を得て移転することも可能である．しかし，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 [8]．

グローバルに事業を展開する企業にとって，個人データの国際間の流通を規制されることは，事業の発展に多大な影響を及ぼすこととなる．たとえば，日本企業が EU 構成国の企業を買収した場合，原則として買収先企業の幹部社員や従業員の人事データを日本本社に送ることがでず，また消費者などのデータを送信することができない．そうなれば，買収した企業の管理を行うことはできず，単に財務諸表に売上利益を連結するにとどまるのである．

わが国は，EU 域内に事業を展開する日系企業が，EU データ保護指令 26 条に規定された例外的措置をいかに利用するか，という議論を行うのではなく，欧州委員会により「十分性」を認定される個人データ保護法制を定立する必要があろうことは自明である．

2.3　EU データ保護指令とわが国の個人情報保護法の相違

1998 年 10 月 24 日，EU データ保護指令が発効した時，わが国には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 データ保護指令が第三国に求める保護の「十分性」など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．

同時に，1999（平成 11）年 6 月，住民基本台帳ネットワーク実現に向けた住民基本台帳法改正の際，当時与党であった自由民主党，自由党，公明党の 3 党間で民間部門の個人情報保護法を 3 年以内に法制化することについての確認がなされた．このような国内外の経緯から，2003（平成 15）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が成立し，同年 5 月 30 日に一部施行された．

わが国が，現行の個人情報保護法制により，EU データ保護指令第 29 条作業部会に「十分性」評価を申請した場合，どのような評価を得るのであろうか．

（1）開示請求

わが国の個人情報保護法において，本人の開示請求に関する規定は，同法 25 条（開示）に規定されているが，同法の中では「個人情報取扱事業者の義務」として位置付けられている．開示の求めに対し，本人の情報を開示することを事業者の義務としているに留まり，開示の求めを本人の「権利」として規定していない [9]．

一方，EU データ保護指令においては，アクセス権（right of access）としてデータ主体の権利を規定している（指令 12 条）．これは，データ主体が保存されているデータに関する情報を取得し，修正，消去するなどの権利としており，「加盟各国は各データ主体に管理者から得る権利を保障しなくてはならない」ものとしている．さらにデータの主体に対し，与えられる権利として，異議申立権（指令 14 条），自動処理された個人決定に服さない権利（指令 15 条）がある．さらに一部の例外を除いては，構成国が設けなければならない監督機関に対し，データ処理の適法性に関する捜査請求をすることができる（指令 28 条 4 項）．

このように EU データ保護指令は，開示請求などを本人の「権利」として規定しており，本人が法のエンフォースメントに関与できる点が，わが国の法制と大きく異なる [10]．

（2）監督機関

わが国の個人情報保護法には監督機関に該当する概念はない．しかし，5,000 件を超える個人データを保有する個人情報取扱事業者に対し，主務大臣が報告，助言，勧告，命令等により関与することになっている．なお，公的部門を対象とした監督機関は存在しない．

一方，EU データ保護指令においては，監督機関の設置を規定している（指令 28 条）．この監督機関は公的部門および民間部門の双方を監督の対象とするため，独立性が強く，「個人情報保護法における主務大臣とは基本的に異なる」[11] 機関である．

（3）特別カテゴリーのデータの処理

EU 指令では，「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の処理」[12] を，原則として禁止している（指令 8 条 1 項）．しかし，わが国の個人情

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	5,000 件を超える個人データを超える事業者
情報の種類	センシティブ情報の収集制限	情報の質による法律上の義務の違いはない
開示請求等	権利（right）	事業者の義務
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	独立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

（注）各種資料により筆者作成

報保護法における定義規定では，個人情報，個人データ，保有個人データという定義が規定されているが，その内容や性格により，取扱いに違いはない．

その他にも表１のように，わが国が現行法制度のまま，EU データ保護指令 29 条作業部会に「十分性」評価の申請を行った場合に，十分性を認められないであろうと懸念されるいくつかの相違があるが，本稿では誌面の関係から以上にとどめる．しかし，EU 構成国との自由な情報流通に主眼を置き，今後わが国における新しいプライバシー保護法制を検討するのであれば，このような EU データ保護指令との相違の検討は必要であろう．

３．情報の不正取得者への法的制裁

3.1　情報流出事件に関する企業防衛上の課題

近年，企業による情報流出事件が相次いでいる．例えば 2009（平成 21）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では，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[13]．近年，顧客情報の窃取が目立つのは，企業が保有する様々な情報の中でも，特に個人情報が換金性に優れ，窃取後の利用価値が高いためと思われる．

企業による個人情報の漏えいは，本人のプライバシーを侵害し，また二次的な被害を引き起こす可能性が高い．また情報の保有者である企業に対し，多大な影響を与える．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の経済的リスク，プライバシー侵害を根拠とする本人からの訴訟リスク，個人情報の保護に関する法律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，そして情報漏えいによる損失が会社法上の取締役の内部統制システム構築義務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．

一方で，企業が情報の不正取得者に対峙する場合，有体物を中心とする体系を取ってきたわが国の刑法では，無形の情報の不正取得行為への刑事罰による対応が難しい．また，2003（平成）年に成立した個人情報保護法は，企業が保有する個人情報の不正取得者への法的制裁を規定していない．

「情報」を客体として，その不正取得に刑事罰を設けている法律は，不正競争防止法である．同法は 2003（平成 15）年の改正により，営業秘密侵害罪が加入された．しかし客体となる情報は，「秘密管理性」「有用性」「非公知性」の３要件を充足する営業秘密と定義されているが，

特に秘密管理性要件が厳しいため，その適用は限定的であるし，そもそも経済法に個人データ保護の役割を期待することの是非も考えられる．

本項では，情報の不正取得への刑事罰導入の経緯を整理し，現行法制度上の問題を検証するとともに，企業が保有する個人情報の不正取得者への法的制裁のあるべき仕組みを探究する．

3.2　情報の不正取得への刑事罰導入の経緯

わが国では，1950 年代以降，産業スパイ事件が多発した．情報の財産的価値が注目を浴び始めたこの時期，情報の不正取得への刑事罰の導入を求める主張があり，1974（昭和 49）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．

消極論としては，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もの，企業の中で法的な保護を受けたい情報は無体財産制度を活用すべきとするもの[14]，また立法技術上，企業秘密の侵害の外縁の規定が困難とするもの，などがあった．さらに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[15]，などの意見があったようである．

逆に積極論は，秘密が化体した媒体自体を侵害せず，情報のみを侵害する行為について，窃盗，業務上横領の成立を肯定することは困難であること[16]，また企業が保有する情報の中でも，特許権，意匠権，著作権といった知的財産権による保護の対象となる情報はごく一部であり，さらに特許法は登録を前提とした権利付与であるため，登録までに時間がかかること，などの法制度上の問題を指摘した．結果として同条は継続検討となった．

その後，「GATT ウルグアイラウンド」において交渉項目として営業秘密の保護が取り上げられ，国際的要請が高まったことなどから，営業秘密の不正な取得・使用・開示行為を「不正競争」と定義し，差止め，損害賠償，信用回復措置請求権による民事的保護を定めた改正不正競争防止法が 1990（平成 2）年 6 月 22 日に国会で可決成立し，同年 6 月 29 日に公布された．しかし刑事罰についてはその加入を見送られた．

3.3　アメリカの経済スパイ法とわが国の営業秘密侵害罪の創設

一方，アメリカでは外国政府機関が関係するスパイ行為，および個人または企業を利するためのトレード・シークレットの侵害行為に対する刑法上の制裁を目的する最初の連邦法として，1996 年 10 月 11 日，経済スパイ法[17]が発効し，これにより連邦法典第 18 典に経済スパイ罪[18]（Economic espionage）とトレード・シークレット窃盗罪[19]（Theft of trade secret）が新設された．

経済スパイ法におけるトレード・シークレットの定義は，「保有者がその秘密性を保持するための合理的な措置をとっており，かつその情報が公然と知られておらず，一般的に合法的手段で確認することができない情報であり，現実にも潜在的（actual or potential）にも経済的価値を有する情報」（法 1839 条 3 項）と規定されている．

その対象となる行為は，経済スパイ罪においては「(a)意図的もしくは認識して，外国政府（foreign government），外国機関（foreign instrumentality），もしくは外国係官（foreign agent）を利する（benefit）ため」にトレード・シークレットの窃取を行う行為等であり，トレード・シークレット窃盗罪においては，「意図的もしくは明白な認識のもと，トレード・シークレットを不正取得する行為等」に適用される．

どちらも非親告罪である．

経済スパイ法はインターネットやコンピュータの発達に対応し，「トレード・シークレットを窃取する行為からトレード・シークレットを保護する」[20] ことが意識されている．経済スパイ法における窃取などの行為の客体は「情報」であり，さらには経済的価値には潜在的価値を含むことから，保有者による合理的な秘密管理措置をとっている非公知情報であれば，すべての情報がその保護対象となりえる．トレード・シークレットの定義が広く，そのうえ法に抵触する客観的行為も広く，不正取得・漏えい行為などはもとより，コピー，複製，スケッチ，模写，ダウンロード，アップロードする行為，さらに許可なく獲得，譲渡等されたことを知りつつ，受領，購入する行為，犯罪の企画，共謀，予備などの行為類型が含まれる．

立法当時は湾岸戦争終結後であり，世界各国の諜報機関の存在価値が低下し，その対象がアメリカの経済情報の入手に向いている状況であった．アメリカ政府の保有する軍事的情報やアメリカ企業が保有する最先端の技術情報は，北朝鮮での核兵器開発プログラムなどに利用価値が高い状況下にありながら，アメリカは情報を保護するための連邦での刑事上の法制度が未整備であった．そのような背景から連邦トレード・シークレット法成立の意義は大きいと評価されている [21]．さらに，2001 年 9 月 11 日アメリカにおける同時多発テロ以降，財産的情報を目標としているテロリストのスパイ活動が，アメリカ合衆国の経済競争力の低下と，テロの脅威を増大させる状況に対応する効果的な法制度として機能することが期待されている [22]．その上，日本人研究者がアメリカ司法当局により経済スパイ法違反容疑を問われ，国際問題に発展した事件（後述）を挙げ，「経済スパイの脅威はフランス，イスラエル，中国，ロシア，イラン，およびキューバ各国政府機関とともに日本」もその脅威と指摘されている [23]．そしてこのような外国政府機関又は外国企業の経済スパイによるアメリカ合衆国の損失は推定で 630 億ドルと見積もることができ，米国経済にとって大きな影響を与えているとも指摘されている [24]．

そのような中，アメリカで働く日本人研究者の 2 つの事件が起き，日米間の営業秘密（トレード・シークレット）保護法制の不整合が顕在化した．

第一の経済スパイ事件 [25] は，アメリカのクリーブランド・クリニック財団ライナー研究所に勤務し，アルツハイマー病の研究をしていた岡本卓氏（当時）が，1999 年 7 月，日本の理化学研究所に転職を決めた際，同研究所から遺伝子試料等を持ち出し，これをカンザス大学の芹沢宏明助教授（当時）に送ったことにつき，両研究者が経済スパイ法（Economic Espionage Act）および連邦贓物法（National Stolen Property Act）違反容疑で起訴された事件である．

本件はその後，アメリカ政府の請求により東京高等裁判所において日米犯罪者引渡し条約に基づく引渡し審査が行われたが，2004（平成 16）年 3 月 29 日，東京高裁は岡本卓氏が試薬を持ち出した際に，転職先である理化学研究所の利益に資することを意図し，またはこれを知っていたと疑うに足る相当な理由はなく，アメリカ法に基づく犯罪の嫌疑が認められないとし，引渡しをしないとした．

また，この年は別の日本人科学者による第二の経済スパイ事件 [26] も発生している．本件は，ハーバード大学で臓器移植の際の拒否反応を抑える免疫抑制剤の開発に役立つ遺伝子の研究をしていた中国国籍の夫が，1999 年 10 月テキサス大学に転職する際，ハーバード大学の許可を得ずに当該試料を送ったことにつき，同研究員

と日本国籍で元ハーバード大学研究員の妻が，経済スパイ法および連邦贓物法違の容疑で起訴された事件である．

このように，広い定義規定，行為態様，さらに非親告罪による運用を規定する経済スパイ法は，アメリカ司法当局による恣意的に運用されないのだろうか，という疑問がある．

これらの事件を契機として[27]，営業秘密を対象とする刑事罰の導入等を内容とする不正競争防止法の一部を改正する法律が成立し，2004（平成16）年1月1日に施行された．その後，同法は改正を重ね，現在の営業秘密侵害罪に至っている．

営業秘密侵害罪は，営業秘密の不正取得・領得・不正使用・不正開示のうち，一定の行為について，10年以下の懲役又は1,000万円以下の罰金（又はその両方）を科すこととしている．いずれも，「不正の利益を得る目的」又は「営業秘密の保有者に損害を加える目的」で行う行為が刑事罰の対象であり，報道，内部告発の目的で行う行為は処罰の対象外である．

3.4　営業秘密（トレード・シークレット）の保護に関する日米比較

わが国とアメリカの営業秘密（トレード・シークレット）に係る法を比較すると，まず民事においては，アメリカの多くの州が採択している統一トレード・シークレット法[28]とわが国の不正競争防止法上の営業秘密の民事的保護に大きな違いは存在しない．判例上では，アメリカが情報の正当な保有者，明示的または黙示的な保有者・取得者間の契約または信頼義務にその判断の主眼が置かれており，秘密管理性に関しては「合理的な努力」としているのに対し，日本の判例では秘密管理性，特に客観的認識可能性に主眼が置かれている点，またアメリカは裁判所が下す損害賠償額の2倍を上限とする懲罰的損害賠償請求権，および利益返還請求権をおいている点が，日本の法制度との違いである．

これに対し，刑事的制裁に関しては，その適用の範囲に大きな違いがある．アメリカにおける州際または外国へのトレード・シークレットの移動は，経済スパイ法が適用される可能性が高いが，その客体となる情報の有用性の定義は「現実又は潜在的な経済的価値」とされており，現在使用していない情報や現実的には経済的価値を有しないが，潜在的価値を有する情報についても積極的に有用性が認められる．したがって，例えば既に退職した従業員リストや，古い取引先リストなど，当該情報保有者にとって現実的に経済価値を有しない情報であっても，他者にとっては潜在的価値がある場合，これを州を超えて移動したり，または国外に移動したりする場合には経済スパイ法違反として処罰の対象になる場合がある．また秘密管理性についても，アメリカは秘密を保持する「合理的な措置」を要件とするが，わが国の場合は客観的認識可能性（当該情報にアクセスしたものに当該情報が営業秘密であることを認識できるように，例えば「秘密」などの表示がされていること）を要件としており，外形的・客観的な管理が必要である．わが国の営業秘密に関する裁判例のうち，秘密管理性について判断した81件の中で，秘密管理性を肯定したものは23件[29]（23.9%）にとどまっており，この要件が厳格に判断されていることがわかる．さらに，アメリカの経済スパイ法は非親告罪であるのに対し，わが国の場合は親告罪である．

このように，わが国における顧客リスト等の大量漏えい事件への刑事法上の処罰は，アメリカに比べてその適用が厳しい．この差は，わが国企業のアメリカにおける経済活動や，わが国研究者の研究活動への委縮効果を生んでいるように思う．

表 2　日米の営業秘密（トレード・シークレット）の刑事罰

	日本（営業秘密侵害罪）	アメリカ（経済スパイ罪）
法　律　名	不正競争防止法	Economic Espionage Act
定　義	• 秘密管理性 （客観的認識可能性・アクセス制限） • 有用性 • 非公知性	• 秘密を保持する合理的な措置 • 現実又は潜在的な経済的価値 • 非公知性
目的要件	図利加害目的	図利加害目的
客　体	情　報	情　報
刑　事　罰	個人：10 年以下の懲役又は 1000 万円以下の罰金 法人：3 億円以下の罰金	個人：15 年以下の禁固，50 万ドル以下の罰金 企業：1,000 万ドル以下の罰金
親告罪・非親告罪	親告罪	非親告罪

（注）各種資料により筆者作成

一方で，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限界がある．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．

3.5　イギリスの 1998 年データ保護法におけるデータ不正取得者への刑事罰

わが国において，顧客リストの不正取得への刑事的制裁は，長年にわたって「法制度上の間隙」といわれてきた．例えば，アルバイト大学院生が 21 万件余の住民基本台帳データを不正に取得して名簿業者に売り渡した宇治市住民基本台帳データ大量漏えい事件では，自己所有の光ディスクにコピーして持ち出したために，当該大学院生は窃盗罪などの現行刑法上の罪に該当せず不起訴となった．また，ソフトウェア開発会社の従業員が委託元銀行の 2 万人余の顧客データを持ち出し名簿業者に売り渡したさくら銀行顧客データ不正取得事件[30]では，銀行顧客データの不正取得行為に関しては，自己所有のフロッピーディスクにコピーして持ち出したため，横領罪などの現行刑法上の罪に問うことができず，業務上預かり保管中の書類 4 枚をコピーし売却する目的で持ち出した行為につき，業務上横領罪で処罰された．このような事件から考えると，現行法制度が情報の不正取得への本質的な法実現性を担保しているとはいいがたい．

このような問題意識から，企業が保有する個人情報の不正取得への現行法制上の唯一の刑事罰である営業秘密侵害罪について，その創設の経緯や適用を概括してきた．しかしその適用は，企業における秘密管理性が厳しく問われ，実効性に欠ける．さらに経済法である不正競争防止法を，プライバシー保護のために活用することに，そもそも無理がある．個人情報の不正取得者への刑事罰の導入を検討すべきではないだろうか．

イギリスの 1998 年データ保護法（Data Protection Act 1998, c. 29.）（1998 年 7 月 16 日女王の裁可，2000 年 3 月 1 日施行）は，そのような議論に示唆を与えてくれる．同法は，情報の詐取等の行為への刑事罰を設けている．同法 55 条は，個人データの違法な取得等（Unlawful

obtaining etc. of personal data.）として，次のように規定している．

「(1)人は，データ管理者の同意を得ずに，故意又は過失によって，次に掲げる行為を行ってはならない．
(a)個人データ又は個人データに含まれる情報の取得又は開示．
(b)個人データに含まれる情報を他の者に開示させること」

同法では，上記への違反行為を犯罪としている((3)項)．また，(1)項に違反して取得した個人データを販売し，または販売を申し込み，もしくは販売の広告を行うことを犯罪と規定している((4)－(6)項)[31]．

同法の定義規定では，個人データは，「生存する個人に関連する情報であって，その情報自体で，あるいはデータ管理者が保有するほかの情報を加えることで個人を識別できる情報で，個人に関する意見の表明や，データ管理者その他の人の評価を含む」と規定されている．したがって，本人に対する評価情報や意見を含んでおり，これらの情報について，データ管理者の同意を得ずに取得，開示などを行う行為は刑事罰の対象となる．

わが国において，個人情報窃盗罪を創設する場合，法に対する過剰反応と，情報の自由な流通を阻害する萎縮効果を起こさないように考慮する必要がある．したがって，①明確な故意犯を対象とすること，②図利加害目的であること，③個人データを保有する事業者の同意を得ていないこと，の３点を構成要件として処罰規定を加入してはどうか．

４．その他の国内問題

以上，検討してきた問題以外にも，わが国の個人情報保護法は様々な課題を抱えている．第一は共通番号制導入の議論である．2009（平成21）年６月23日に閣議決定された「経済財政改革の基本方針2009～安心・活力・責任～」において，「子育て等に配慮した低所得者支援策」として，「給付つき税額控除等」が提言されている[32]．国民個々人の所得と納税額を把握し，低所得者への税金の還付を行うことを主たる目的として，共通番号制の導入とともに，第三者機関の創設が議論されている[33]．

一方，5,000万件にも及ぶ「消えた年金記録」問題[34]，100歳を超える高齢者の存否の把握が十分になされていないという問題[35]など，近年，行政における情報管理の稚拙さが問題視されており，共通番号にこれらの情報を付加することで，行政における情報管理の問題を解決すべきとする議論もある．

このように，行政が保有する情報を一元的に管理することは，行政の効率化の観点からも有益であり，第三者機関の創設とともに，各省庁の計画に明記されている状況である．しかし1960年代から社会保障番号を税務に使っているアメリカでは，他人の社会保障番号（Social Security Number, SSN）を不正に利用してクレジットカードを作成したり，借金をしたりという「成りすまし」被害が少なくない．また，年金記録などを付加する場合は，医療機関での治療内容や病歴などの情報と紐付くことになり，さらに深刻なプライバシー侵害の可能性が高まるとともに，国家による国民の過剰な管理も懸念されている．

さらに民間部門においては，情報化の進展がマーケティング技術を発展させ，以前に増して個人情報の利用価値が増している．例えば，イン

ターネット広告の一手法として，「行動ターゲティング広告（Behavioral Targeting AD, BTA）」が注目を集めている．この手法は，ユーザーが閲覧したウェブサイトや検索サイトで入力したキーワードなどの情報から趣味や趣向を分析し，ユーザーにマッチした広告を表示する手法であるが，趣味や趣向の分析はユーザーの許可なく行われている．

その上，企業による従業員の監視技術が進歩し，オンライン・モニタリング[36]，RFID（Radio Frequency Identification）[37] や GPS（Global Positioning System）による従業者の行動監視などのモニタリング技術が進歩している．

現行の個人情報保護法制は，行政や企業におけるプライバシー保護のために，十分であるとは言い難い．わが国は現行の個人情報保護法制を見直し，プライバシー保護の新たな枠組を構築しなければならない．

5．むすびにかえて ── 新たなプライバシー保護法制 ──

前述のように，わが国のプライバシー保護の枠組みは，多くの面で様々な課題を抱えている．これを解決するためには，現行の個人情報保護法制（個人情報の保護に関する法律，行政機関の保有する個人情報の保護に関する法律，及び独立行政機関の保有する個人情報の保護に関する法律）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．

具体的なプライバシー保護の法的枠組は次のようなものである．すなわち現行の個人情報保護３法を廃止し，官民双方を対象とし，本人の権利保護を目的としたプライバシー保護法を定立すべきであろう．同法は本人が開示，訂正，削除などの出訴可能な請求権を規定し，一方で企業の情報の流通と利用を促進し，また不正に情報を取得する者に対する刑事罰を創設すべきであろう．また官民双方のプライバシー保護を監視する権限を有した独立監視機関を創設する必要があろう．

この新たなプライバシー保護法制の定立および独立監視機関の創設とともに，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べきであろう．

さらに権利の主体である国民が自らの権利を主張し，また他者の権利を尊重するためには，プライバシーの権利に関する教育活動を行う必要もあろう．

2010 年 11 月 1 日に，社会的責任の国際規格である「ISO SR 規格（ISO26000）」が発効した．プライバシー権は，ISO SR 規格の 7 つの中核課題の一つ，「人権」における主要な要素である．ISO SR 規格は，ある意味でわが国がその定立を主導した．わが国は今，CSR 先進国として世界の先頭を走ろうとしている．そのような中，わが国は EU から「基本権としてのプライバシー保護が十分でない国」との評価を受けていることは，わが国の国益にとってのマイナスでる．

わが国は，EU データ保護指令 26 条の例外措置をいかに利用するかを考えるのではなく，欧州委員会への十分性評価の申請を行い，EU データ保護指令第 29 条作業部会により「十分なレベルの保護（adequate level of protection）」の国として評価され，承認を受けるべきだろう．これは，EU 構成国からの情報の移転を容易にし，経済の活性化にも寄与することとなろう．

注

1） 2010（平成 22）年 5 月，筆者がフェローを務める日本経営倫理実践研究センターの会員企業 53 社にアンケートによる調査を行ったところ，社名非公開を条件として 21 社が回答した．

2） 堀部政男　プライバシー・個人情報保護の国際的整合 所収 堀部政男編著（2010）．プライバシー・個人情報保護の新課題　商事法務 pp.52．2009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「十分性認定手続（Adequacy finding procedure）」のプレゼンテーションとして紹介されている．

3） 2010（平成22）年10月16日に上智大学で行われた日本経営倫理学会第18回研究発表大会において，筆者が「共通番号制導入と新たなプライバシー保護法制の提案」と題した研究報告を行い，EUにおけるわが国の評価を紹介したところ，傍聴していた多くの研究者，実務家が同様の感想を述べた．

4） 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. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML（2010年10月15日確認）．
EUデータ保護指令に関する評論は数多いが，主に堀部政男（2002）．個人情報保護法の提唱と議論　pp.7～10，新保史生（2000）．プライバシーの権利の生成と展開　成文堂　pp.285～288などを参考にした．

5） EC条約189条の規定では，「規則（regulation）」は自動的に全加盟国の国内法の一部となり，「指令（directive）」は全加盟国が指令に基づき国内法として立法義務を有し，「決定（decision）」は特定の加盟国を拘束し，そして「勧告（recommendation）」，「意見（opinion）」は加盟国に拘束力を有しない．

6） EUデータ保護指令第25条第1項および第26条第1項の邦訳は，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．

7） 堀部・前掲注（2）p.49．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「十分性」の認定を行い，また2009年12月1日に，イスラエル（Israel）及びアンドラ（Andorra）について十分性を認める意見を採択した，と紹介している．

8） 消費者庁（2010）．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　pp.25-29，「（3）日系企業の対応状況」を参考にした．

9） ただし学説上，わが国の個人情報保護法25条1項の解釈は，開示等の求めに関する具体的権利性の肯定説と否定説がある．否定説としては，「個人情報取扱事業者の法律上の義務である」（園部逸夫（2003）．個人情報保護法の解説 ぎょうせい　p.156およびp.159），「裁判上の請求権を付与したものと解することはできない」（鈴木正朝（2010）．個人情報保護法とプライバシーの権利――「開示の求め」の法的性格 所収 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 p.89）とする説などがあり，また肯定説としては，法案審議において細田国務大臣が立法者意思として権利を付与した旨を答弁していることなどを根拠として「立法者意思に照らして具体的権利性を肯定すべきである」（岡村道久（2009）．個人情報保護法 商事法務　p.270）とする説などがある．なお，東京地方裁判所　平成19年6月27日判決（判時1978号p.29）では開示の求めについて権利性を否定している．

10） わが国においても，行政機関個人情報保護法，及び独立行政法人個人情報保護法は本人の開示請求権として権利構成しており，本人が情報開示を請求し，適切な開示が行われなかった場合には，行政不服審査法に基づく不服申立てを行うことができる．

11） 堀部・前掲注（2）p.44．

12） 前掲注（6）．

13） アリコジャパンによる2009（平成21）年11月11日「お客様情報の流出について――不正使用の監視を強化――」を参照．http://www.

alico.co.jp/about/press/09_1111.pdf（2010年10月15日確認）

14） 佐久間修(1991)．刑法における無形的財産の保護　成文堂　p.1以下.

15） 特に当時は消費者運動，公害運動が盛んであり，これらの運動を抑止する効果があると主張されたようである.

16） 山口厚(1986)．企業秘密の保護　ジュリスト第852号　p.48.

17） Economic Espionage Act of 1996, 18 U. S. C. §§1831-1839（2006）.

18） 18 U.S.C. §1831.

19） 18 U.S.C. §1832.

20） 本法署名時のクリントン大統領の声明．アメリカ司法省はウェブサイトで同声明を公表している．http://www.usdoj.gov/criminal/cybercrime/usamay2001_6.htm（2010年10月15日確認）

21） Michael T. Clark （1997）. *Economic Espionage, The Role of the United States Intelligence Community*, 3 J. Int'l Legal Stud., p.254.

22） Susan W. Bernner and Anthony C. Crescenzi（2006）. *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 Hous. J. Int'l L, p.392.

23） *Id.*, at 406.

24） David J. Loundy （2003）. *COMPUTER CRIME, INFORMATION WARFARE, AND ECONOMIC ESPIONAGE*, p.546.

25） United States v. Takashi Okamoto, Hiroaki Serizawa,（N. D. Ohio, May 8, 2001）.
R. Mark Halligan の Website 'THE TRADE SECRETS HOMEPAGE' 参照.
http://tradesecretshomepage.com/indict.html#_Toc9924990（2011年2月20日確認）

26） United States v. JIANGYU ZHU, a/k/a Jiang Yu Zhu and Kayoko Kimbara（June 19, 2002）.

27） わが国は国家として知的財産戦略を樹立し，知的財産権の保護や有効活用策を検討することを目的に，首相直属の私的懇談会である「知的財産戦略会議」を設置した．同会議は，2002（平成14）年7月3日，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た．同委員会が2003（平成15）年2月に公表した報告書では，「情報のデジタル化や人材の流動化により，現行刑法の制定当時では想定されなかった情報（無体物）である営業秘密自体の不正取得等の紛争が増大しており，また，営業秘密の価値の増加により，これらの行為による被害も甚大化している」状況から，違法性の高い行為について刑事罰を導入すべきと主張している.

28） Uniform Trade Secrets Act. 諸州のトレード・シークレット法の違いが州際取引にもたらす不都合を解消する目的で，統一州法委員会全国大会（the National Conference of the Commissioners on Uniform State Law）により1979年，統一トレード・シークレット法草案が採択され，その後修正を経て，1985年8月8日現在の統一トレード・シークレット法が採択された.

29） 経済産業省 営業秘密管理指針　2010年4月9日改定版　p.28.

30） 東京地判平成10年7月7日判時1683号p.160.

31） ただし，犯罪の予防又は犯罪捜査に必要な場合，法令に基づく場合又は裁判所の命令がある場合，公共の利益となる場合などは適用を除外している.

32） 閣議決定 経済財政改革の基本方針2009～安心・活力・責任～ 2009年6月23日，p.13. http://www.kantei.go.jp/jp/singi/keizai/kakugi/090623kettei.pdf（2010年10月15日確認）.

33） 国家戦略室 社会保障・税に関わる番号制度に関する検討会　中間取りまとめ　2010年6月29日．http://www.npu.go.jp/policy/policy03/pdf/20100629/20100629_syakaihosyou_6_haihu.pdf（2010年10月15日確認）.

34） 2007（平成19）年5月，国会における社会保険庁改革関連法案の審議中に，社会保険庁（当時）がコンピュータ入力した年金記録にミスや不備が多いことが指摘され，その結果，基礎年金番号に統合されていない年金記録が約5,000万件あることが判明した.

35） 2010（平成 22）年，100 歳を超える高齢者の行方不明が相次いで発覚した事件．個人情報保護法の目的外利用の禁止により，福祉課や介護保険課などが把握している個人情報を，互いに照会できないと説明する自治体もあり，個人情報保護法の過剰反応と指摘された．

36） 社内ネットワークを介した，企業の情報資源や外部ネットワークへのアクセス状況を記録・解析する技術．

37） 電波を利用して人や物を認識する非接触型の自動認識技術．アンテナ付き IC チップを社員証カードなどに埋め込み，入退室情報などを収集することができる．

参考文献

［1］堀部政男（1980）．現代のプライバシー　岩波書店．

［2］堀部政男編著，高野一彦他著（2006）．インターネット社会と法　第 2 版　新世社．

［3］堀部政男編著，高野一彦・鈴木正朝他著（2010）．プライバシー・個人情報保護の新課題　商事法務．

［4］新保史生（2000）．プライバシーの権利の生成と展開　成文堂．

［5］園部逸夫（2003）．個人情報保護法の解説　ぎょうせい．

［6］岡村道久（2009）．個人情報保護法 商事法務．

［7］石井夏生利（2008）．個人情報保護法の理念と現代的課題 ── プライバシー権の歴史と国際的視点　勁草書房．

［8］鈴木正朝（2004）．個人情報保護法とコンプライアンス・プログラム ── 個人情報保護法と JIS Q 15001 の考え方　商事法務．

［9］デジタル・フォレンジック研究会監修，小向太郎他著（2010）．実践的 e ディスカバリ ── 米国民事訴訟に備える　エヌティティ出版．

［10］Alan F. Westin （1967）．*Privacy and Freedom*, 7.

［11］佐久間修（1991）．刑法における無形的財産の保護　成文堂．

［12］田中宏司（2007）．CSR の基礎知識　日本規格協会．

［13］水尾順一，田中 宏司（2004）．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．

［14］水尾順一（2005）．CSR で経営力を高める　東洋経済新報社．

［15］Beauchamp, T. L. and Bowie, N. E. eds.（1997）. *Ethical Theory and Business*, 5th ed., Prentice Hall.（加藤尚武訳（2005）．企業倫理学 1　倫理的原理と企業の社会的責任，梅津光弘訳（2001）．企業倫理学 2　リスクと職場における権利・義務，中村瑞穂訳（2003）．企業倫理学 3　雇用と差別／競争と情報　晃洋書房．）

［16］Lippke, R. L.（1995）. *Radical Business Ethics*, Rowman & Littlefield.

［17］亀井俊明，亀井克之（2009）．リスクマネジメント総論 増補版　同文舘出版．

［18］吉川吉衛（2007）．企業リスクマネジメント ── 内部統制の手法として ──　中央経済社．

（掲載決定日：2011 年 2 月 4 日）