ネットワーク社会における個人情報・プライバシー保護のあり方

Data Protection and the Right to Privacy in the Networked Society

新保史生 Fumio SHIMPO

アブストラクト 法令遵守への対応にあたって、その基準が一般に分かりづらいと考えられがちな個人情報・プライバシー保護への対応について、両者の違いを明確にした上で、マネジメントシステムの活用のある方をプライバシーバイデザイン (PbD) やプライバシー影響評価 (PIA) を通じて考察する。いわゆるビッグデータの取扱いへの対応については、自主規制による取組みとしてライフログ活用サービスにおける配慮原則及びスマートフォンプライバシーイニシアティブを取り上げ、今後の我が国の個人情報保護制度のあり方を提示する。

キーワード 個人情報, プライバシー, PbD, PIA, PETs, ライフログ, ビッグデータ

Abstract The compliance issues with respect to data protection and the right to privacy have been regarded as a very problematic and complex, and even unintelligible issue. In this paper, I will explain the precise difference between data protection and the right to privacy. Furthermore, I will focus on the *raison d'être* of the management system regarding the protection of personal information by considering "privacy by design" (PbD) and "privacy impact assessment" (PIA). With regard to the correspondence of so-called "big data" usage to current legal schemes worldwide, I will introduce the MIC life-log handling principles and smartphone privacy guidelines. Finally, I will offer a solution to the current concerns of the Japanese data protection legal system that will appropriately address to the above-mentioned issues.

Key words Personal Information, Privacy, PbD, PIA, PETs, Life Log, Big Data

1. 問題の背景

情報機器の発達とインターネットの進化により、日々新たな技術開発とそれらを利用したサービスが提供されるに伴い、個人情報・プライバシー保護を巡る新たな課題が生じている。しかし、「個人情報」と「プライバシー」の違いを考慮せずに対応することにより、本来「必要な対応」が見落とされる一方で、「必要ではない対応」がなされるという問題が生じている。とりわけ、個人情報保護至上主義ともいえる過剰な対応、不十分な法令解釈に起因する事業の取りやめや参入への躊躇など、法令遵守への取組みに起因する事業への萎縮効果の顕在化、法のグレーゾーンに乗じた不適正な情報の取扱いや消費者の不知につけ込んだ野放図な個人情報の取扱い、本人同意によりいかなる情報の取扱いも許容されるといった誤った認識とそれを後押しするような法令の問題も指摘⁽¹⁾されており、法令遵守義務とその目的が十分理解されていないがゆえに生じている問題がある。反面、自分だけは情報漏えいを発生させないという根拠がない自信や、法令遵守への取組みを軽視しても責任を問われないといった責任感の欠

如、肝心の対策が何ら実施されずに主観的 (自己) 満足にすぎない情報セキュリティ対策、中身がないキャッチフレーズの対応 (例: 情報セキュリティ対策を十分に検討することなく BYOD⁽²⁾ を勧められるがままに導入するなど) 等、法令遵守以前の社会的・道義的責任から考えなければならない問題もある。

これらは、法規制の有無、適用法令の把握、適切な法解釈によって解決されることが望ましいが、近時の技術開発の進展やネットワークの発達により、環境変化への客観的対応の必要性和現状に即し時宜に応じた対応が求められている。

なお、個人情報保護法の過剰反応を巡る問題については、情報社会における制度的な課題を総合的に検討した上で理解する必要があるが、その点については、本会の辻井論文⁽³⁾を参照されたい。

本稿では、法令遵守への対応にあたって、その基準が一般に分かりづらいと考えられがちな個人情報・プライバシー保護への対応について、プライバシーと個人情報の違いを明確にした上で、マネジメントシステムの活用のある方をプライバシーバイデザイン (PbD) やプライバシー影響評価 (PIA) を通じて考え、いわゆるビッグデータの取扱いへの対応について自主規制による取組みとしてライフログ活用サービスにおける配慮原則及びスマートフォンプライバシーイニシアティブを取り上げる。

新保史生 正員 慶應義塾大学総合政策学部
E-mail shimpo@sfc.keio.ac.jp
Fumio SHIMPO, Member (Department of Policy Management, Keio University, Fujisawa-shi, 252-0882 Japan).
電子情報通信学会 基礎・境界サイエティ
Fundamentals Review Vol.6 No.3 pp.199-209 2013年1月
©電子情報通信学会 2013

2. 緩やかな監視

様々な技術を用いるにあたって、個人のプライバシーとの関係において問題が生じる可能性がある場面としては、「監視」技術としての利用が挙げられる。

しかし、監視技術といっても、人々の行動などを当初から「監視・追跡」することをその本来の目的とする「本来の意味での監視技術」と、監視が本来の目的ではないものの新たな技術手段の利用が結果的に監視に結び付いてしまう「事実上の監視技術」に分けて考える必要がある⁽⁴⁾。

これを「緩やかな監視 (Soft surveillance)」の問題として指摘する論考⁽⁵⁾がある。緩やかな監視においては、ある人物が、実際には自らの意思に基づく行為ではないにもかかわらず、監視を受ける環境を自発的に行っているかのような状況が作り出されているとする。換言すれば、強制的な「任意」という矛盾する状況によって、事実上の強制 (Mandatory Volunteerism) による監視を受け入れざるを得ない場面が存在することを意味する。

緩やかな監視の典型例としてこの論考が指摘するのは、コールセンターの担当者と会話をする前に、通話内容の録音の承諾を求めるアナウンスを挙げる。「電話対応の対応の向上のため」録音を行うというものである。不正行為を防止するための監視とは異なり、その目的はあくまで「サービスの向上」ではあるものの、通話内容を録音することに承諾することができない人は、コールセンターに苦情や相談の電話を掛けることができないため、丁寧なアナウンスによって通話内容の録音に任意に黙示の承諾をしているものの、事実上の監視を強制的に受け入れているというものである。

そのほかにも、ネットワークにおけるサービスを利用するにあたっては、「自発的」に、自らの氏名、住所、電話番号、電子メールアドレス、郵便番号、その他オンラインでアクセスするために必要な情報を提供せざるを得ない状況は枚挙にいとまがない。

なお、「監視」という用語を「モニタリング」と表記することもあり、例えば、「個人情報の保護に関する法律」についての経済産業分野を対象とするガイドライン (平成21年10月9日厚生労働省・経済産業省告示第2号) では、「従業者のモニタリングを実施する上での留意点」として、「個人データの取扱いに関する従業者及び委託先の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリング (以下「モニタリング」という。)」と表記している。

個人情報・情報セキュリティに関する分野における両者の使い分けの基準は定かではないが、「監視」よりも「モニタリング」のほうがその侵襲度が低いというイメージで受け止められている感があり、監視という用語を用いることを避けることでプライバシー侵害のイメージを払拭しようとしている感じさえある。「盗聴」と「傍受」の使い分けの違いと同様である。

一方、児童福祉、居宅介護支援、障害者自立支援などの社

会福祉分野においては、その実施状況の把握を、「利用者についての継続的なアセスメントを含む、以下「モニタリング」という。」と表記しており、これら法令用語として用いられている「モニタリング」とは意味が異なる点に注意が必要である。

3. プライバシーへの影響度が高い問題

個人のプライバシーへの影響がある問題は実に多岐にわたる⁽⁶⁾。そのため、個人の人權や権利利益保護の観点から法的課題について検討することが必要な問題も多いことから、それらを統一的・体系的に分類して検討課題を整理することが必要である。そこで、個人のプライバシーへの影響度が高い問題の主たる局面と目的を表にまとめると表1ようになる。表1の内容は、営利目的については民間部門における問題であるが、それ以外の問題は主に公的部門における問題である。左側の利用目的ごとに、具体的にどのような利用局面が想定・存在するのかこちらの表で御確認頂きたい。

また、ネットワークにおいて提供されている様々なサービスを利用することで、本人が知らないうちに「日常的⁽⁷⁾」に様々な情報が取得され利用されプライバシーが明らかにされてしまっていることがある。具体的には、電子メールモニタリング⁽⁸⁾、Webの閲覧状況・アプリケーション・ファイルや印刷等の利用状況モニタリング⁽⁹⁾など、文字どおりの監視。それを実現するクッキー / Webビーコンの利用⁽¹⁰⁾、固有の識別アドレスの監視・追跡、各種ログ解析 (通話、通信、Web)⁽¹¹⁾、KLS (キーロガー⁽¹²⁾) の利用、ネットワーク管理と監視 (ping, nslookup (dig), traceroute (tracert), netstat などの各種コマンド⁽¹³⁾や各種管理 (監視) ツールの利用⁽¹⁴⁾) は、適正に利用されるには問題はないが、監視ツールとして不正に利用されると、スパイウェアの利用と何ら変わらない利用がなされる恐れもある。そのほか、ネットワーク上の個人情報の監視 (P-FindやWhoisなどを用いた個人情報の検索⁽¹⁵⁾) など、ネット上で個人情報を調べる方法もある。

物理的な技術においても、各種センサ、RFID、バイオメトリクス⁽¹⁶⁾、スキャナ⁽¹⁷⁾ (ボディスキャナ等⁽¹⁸⁾)、ロボットな

表1 主な局面と目的

営利目的	マーケティング 目的：行動ター ゲティング広告 等	生活支援、マーケ ティング、利益の 追求、取引の安全 確保	個人の権 利利益保 護	セキュリ ティの確 保
安全保障目的	国防やテロ対策	安全保障		
犯罪捜査目的	犯罪捜査	法執行		
保安・ 警備目的	防犯、施設のセ キュリティ (公 共施設、民間施 設、家屋、空港 や港湾)	治安維持 (公共の 安全確保、公の秩 序維持、侵入・盗 難等の防止)		
防災・ 公衆衛生目的	災害予防、 公衆衛生	防災目的での各種 観測、検疫、公物 管理		

どの利用に伴う個人のプライバシーに及ぼす影響は高まっている。空港の保安システムにおけるX線投影装置(Backscatter⁽¹⁹⁾)については、その利用に伴う健康問題も指摘⁽²⁰⁾されている。バイオメトリクスについては、遺伝子情報の利用が伴う場合には単なる生体情報の利用に問題⁽²¹⁾はとどまらない。

これらを分野別に見ても、ネットワークサービスについては、検索サービス⁽²²⁾、クラウドコンピューティング⁽²³⁾、ソーシャルネットワーキングサービス(SNS)、コンシューマジェネレイティドメディア(CGM)、道路周辺映像提供サービス⁽²⁴⁾、ディープパケットインスペクション(DPI)、デジタル著作権管理(DRM)、位置情報(GPS⁽²⁵⁾)などの利用に伴う問題が増えつつある。

DPIについては、2010年5月30日日付の朝日新聞朝刊1面において、「ネット履歴丸ごと個人用広告に利用 サイト閲覧・検索…接続業者側が分析」という記事が、DPIを行動ターゲティング広告において利用することについて問題を指摘して以降、国内における政府の委員会等における議論は全て取りやめとなった経緯がある。国外における議論⁽²⁶⁾に対して国内における一層の議論の遅れが懸念される。

社会基盤との関係においても、共通番号⁽²⁷⁾、スマートグリッド⁽²⁸⁾、スマートハウスの構築にあたってプライバシー保護の問題は避けて通ることができない。

4. プライバシーと個人情報の違い

4.1 区別の必要性

プライバシーと個人情報保護の問題を考えるにあたっては、両者の違いを認識した上で議論⁽²⁹⁾することが前提となる。両者の区別が不要であるとの考えもあるが、アメリカ法における議論⁽³⁰⁾のように、我が国においてはプライバシーの権利の保護法益や権利侵害の成立要件について詳細な議論がなされてきたわけでもなく、EUのように個人データ保護の観点から情報の適正な取扱いにあたっての手續と規制が十分に整備されてきたわけでもない。その結果、プライバシー・個人情報保護を巡る議論は、EU型の規制と米国型の権利侵害に対する救済の両者が併存する。結果的にいわゆる過剰反応と呼ばれるいびつな個人情報保護法の遵守環境が生じる要因にもなっている。

これは、両者の相違点について分かりづらい側面もあることから、個人情報とプライバシーを同列に論じ、公になっている個人情報であって個人のプライバシーとしては保護することができない情報についても、プライバシーの権利としての自己情報コントロール権の行使が可能であるといった極端な主張を招く結果ももたらしている。

共同体において生活をしている個人は、社会生活を営む上で本人を識別することが不可欠である。他人との識別ができずに契約などの経済活動を行うことはできないであろう。つまり、個人情報は個人を識別する情報として不可欠な情報であるため、本人の身勝手な要求によって適正かつ正当に利用

されている個人情報までもが、自己情報コントロールと称して利用停止や消去されなければならないわけではない。

とりわけ、ネットワーク社会における個人情報プライバシー保護のあり方を考えるにあたっては、この点について確認をしておくことが不可欠である。

4.2 個人情報の定義

個人情報の定義については、個人情報の保護に関する法律(平成15年5月30日法律第57号)第2条において、「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することができるもの(ほか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。」と定義されている。

個人情報保護法では、個人情報の定義を生存する個人に関する情報であつて特定の個人を識別できるものとしている。つまり、個人情報の「種類」や「内容」には着目せずに、あくまで生存性と個人識別性の要件に照らして個人情報に該当するか否かを判断するにすぎない。なお、個人情報保護法の解釈については様々な解釈がなされているが、信頼できる解説⁽³¹⁾を参照されたい。

4.3 個人情報の種類・内容による区別

個人情報は、一般に公開されている情報から他人に知られていない情報に至るまで、その種類や内容によって区別することが可能である。

法律では個人情報の内容について区別していないが、通常、個人のプライバシーや個人情報の問題を考えるときには、おのずと個人情報の内容や種類によって区別しながら一般に考えているといえよう。結果的に法律が定める定義と一般の理解の相違が生じているため、これが、いわゆる過剰反応の根本的な要因となっている。

この誤解を解消するために、図1を御覧頂きたい。個人情報

図1 個人情報とプライバシーの関係

新保史生, “プライバシーの権利,” 憲法入門, 山本順一(編), p.50, 勉誠出版, 東京, 2003.

報は、公になっている情報から、公になっていない情報に至るまで、それぞれ区別することが可能である。区別の方法には様々な方法があると考えられるが、便宜上、①公知、②非公知、③機微な情報に分けて論じたい。

個人情報の種類とプライバシーの保護の対象になる情報の違いを説明する上で、これら三つの種類に個人情報を分けて筆者が論じてきた理由は、信号機の色に例えて個人情報の種類及び内容とその取扱いのレベルについて議論すると、判断基準が難しいと考えられがちな個人情報とプライバシーの範囲を直感的に理解することができると考えているからである。

青色(図の上段)の①公知に該当する情報は、一般に公開されている個人情報である。

個人の氏名など、日頃生活を送る上で特定の個人を識別するために不可欠な情報として様々な局面で利用される情報がこれにあたる。これらの情報を他人に知られたくないと思う場面で、匿名にすることなどはあるものの、その情報は秘密ではなく、あくまで個人の意思によって一般への公開が制限されているにすぎない。

黄色(図の中段)の②非公知に該当する情報は、一般には知られていない情報である。しかし社会生活を送る上で法令に基づいてその提供が義務付けられていたり利用されることがある。社会的な地位や関係において、本人の意思に関係なく利用しなければならない情報がこれにあたる。

最後に、赤色(図の下段)の③機微情報は、他人に知られることを通常は欲しない非公知の情報である。センシティブ情報、または、特定の機微な個人情報と呼ばれるものがこれにあたる。この情報は、本人にとっては他人に知られることを欲しない情報であり、原則として他人に知られることを予定していない情報である。限定的に本人の同意に基づいて利用されることがあるが、その同意は本人の明確な意思表示、つまり明示的な同意に基づいて取扱いが行われなければならない。黙示の同意による利用は適切ではない。

センシティブな情報の取扱いが赤信号にあたる理由は、この情報が第三者に公開されるだけで本人の権利利益が侵害される可能性があるだけでなく、第三者による利用が現実の権利侵害をもたらす可能性が極めて高い情報だからである。例えば、情報が公開されることによって、個人のプライバシーが侵害されるだけでなく、経済的、財産的被害を伴うこともあり得る。また、権利侵害による本人の精神的苦痛、並びに、経済的被害、社会的評価の低下など、個人の権利利益保護の観点からは重大な結果をもたらす可能性がある。

他人に知られていない情報であることから、情報の信ぴょう性も確認できないはずの情報であるため、公開された情報が事実ではなく虚偽の情報に当たる場合には、本人の客観的社会的評価の結果を伴う可能性もあり、その場合はプライバシー侵害ではなく名譽棄損による個人の権利侵害の問題も検討が必要になる場合がある。

4.4 プライバシーとして保護対象となる情報

これらの情報とプライバシーの関係を整理すると、プライバシーとして保護対象となる情報は、基本的には他人に知られることを欲しない非公知の情報がこれに該当するといえる。しかし、他人に知られることを欲しない情報については、人それぞれその感覚が異なることから、その基準は多分に主観的要素による影響を免れない。

判例においても、プライバシー侵害にあたるか否かは、通常人の感受性を基準にして見たときという基準に基づいているにすぎず、どの範囲が明確なプライバシーに該当するか否かは、最終的には個人の主観による判断によって変わるというわざを得ない。

なお、プライバシーの権利の保護法益は諸説あるが、私論⁽³²⁾は以下の三つの領域に保護法益を分けて考えている。

- ① 自らに関する事柄について、外部からの干渉を受けずに自分の意思に基づいて行う「個人の自律」
- ② 他人から干渉を受けたり望まない侵入を受けない隔絶された状態や利益を保護するための「私的な領域」の保護
- ③ 他人に知られたくない個人に関する情報の保護

図1では、それぞれ、①は個人の自律の保障、②は非公知や機微な情報が存在する私的生活領域の保護、③は非公知や機微な個人情報の保護となる。

判例(「宴のあと」事件判決(東京地判昭和39年9月28日判時385号12頁))においては、プライバシーの権利は「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」と定義している。

プライバシー侵害による不法行為の成立要件は、①公開された内容が私生活の事実またはそれらしく受けとられる恐れのある事柄であること、②一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、③一般の人々にいまだ知られない事柄であることを要するとされている。

なお、個人の自律については、これを「自己決定権」と称し、プライバシーの権利とは別個の権利と位置付ける主張が我が国においては有力⁽³³⁾である。その理論的基礎は、トライブ教授の著した『アメリカ憲法⁽³⁴⁾』の15章において述べられた、「プライバシー及び人格の権利」に由来するとされ、本章において、トライブ教授が述べているプライバシーの権利は、プライバシーの権利の構成要素として、人格(personhood)、自律(autonomy)、私事(intimacy)、主体(identity)、尊厳(dignity)といった用語において説明している権利を基礎としている。

判例においても、「エホバの証人」の信者である患者に対して輸血の方針に関し説明をしないで手術を施行して輸血をした医師に対して、患者が輸血を伴う可能性のあった手術を受けるか否かについて意思決定をする権利を奪ったものとして、人格権侵害として民法715条に基づく不法行為責任を負うとする最高裁判決⁽³⁵⁾が下されている。

5. プライバシーバイデザイン という考え方

以上において述べたネットワーク社会におけるプライバシー・個人情報保護をめぐる問題への対策及び定義・権利概念を巡る問題に対して、プライバシー・個人情報保護への取組みも新たな対応が提案されている。その一つが、「プライバシーバイデザイン (PbD)」である。

アプリケーションの実装や情報システムの稼働後に、情報の取扱方法やセキュリティ対策等について、不適正な点を発見した研究者等によるネット上での指摘により、結果的に情報システム等の運用停止や大幅な仕様変更を余儀なくされる事例が散見される。指摘された問題については、事前に精査し問題点を把握しておかなかったことが明らかに疑問に思えるような事例から、複雑な仕様ゆえに問題の発見が困難な事例に至るまで、問題発覚の要因や程度は千差万別である。

とりわけ、情報セキュリティ確保のために最低限必要な措置を講じなかったといった明らかに善管注意義務の懈怠にあたるような事例ではなく、個人のプライバシー保護の観点から情報の取扱方法が不適正であるとの指摘がなされるような事例においては、適切な情報の取扱方法であると確信し何の疑問も持っていなかった研究開発者にとっては、プライバシー侵害にあたるといった指摘は寝耳に水という場合もある。

このような事態に陥らないために、研究開発者が、新たな技術開発に従事するにあたって、その開発過程において法令遵守の問題とりわけプライバシー保護の問題を事前に検討する必要性が高まっていることに異論の余地はないであろう。それを実現する方法として、プライバシーバイデザインの活用が挙げられる。

プライバシーバイデザインとは、プライバシー保護を目的として利用される技術及び対策を、システム設計及びその構築段階から検討・実装し、ライフサイクル全般において体系的かつ継続的に取り組む仕組みである。カナダのオンタリオ州の情報&プライバシーコミッショナー (IPC: Information & Privacy Commissioner) である、アン・カブキアン (Ann Cavoukian) 氏によって提唱された。

その内容は、公正な情報処理 (FIPs: Fair Information Practices) を達成するために、プライバシー保護のための取組みを計画し、それを計画的に実施する上で必要な七つの基本原則と、それを実施するプロセスから構成される。

【PbDの七つの基本原則】

- ① リアクティブ (事後) でなくプロアクティブ (事前)：事後の措置でなく事前に予防
- ② デフォルト設定でプライバシー保護
- ③ 設計時に組み込むプライバシー対策
- ④ 全ての機能に対してゼロサムではなくポジティブサム
- ⑤ エンドツーエンドのセキュリティ：ライフサイクル全体の保護

- ⑥ 可視化と透明性：オープンにする
- ⑦ 個人のプライバシー尊重：個人を主体に考える

PbDは、①「リアクティブ (事後) でなくプロアクティブ (事前)：事後の措置でなく事前に予防」という原則により、事後的な対応ではなく事前対応によってプライバシー侵害が発生する前に、プライバシーへのリスクが発生することを予防することを目的としている。

②「デフォルト設定でプライバシー保護」という原則は、初期設定からプライバシー保護を実施することにより、何もせずにプライバシーが保護されるようにすることが目的である。プライバシー保護のためにどのような技術を利用することができるのか、また、どのように設定すればよいのかといった事柄は、利用者のリテラシーに左右される。そこで、最初からプライバシー保護の仕組みが用意されていれば、利用者にとってプライバシー保護のための対策を考える (悩む) 必要がない。

それを実現するためには、③「設計時に組み込むプライバシー対策」として、システムの仕様を策定する段階からプライバシー保護対策を組み込む必要がある。その際に利用される一つの手段として、プライバシー保護強化技術 (Privacy-Enhancing Technologies: 略称PETs) がある。PETsは、プライバシー保護を向上させるために利用される技術の総称である。プライバシー保護のために、そもそもプライバシー保護の目的を技術手段によって達成しようとするものである。なお、PETsの利用が個人情報保護との関係において明確に示されたのは、ID管理におけるPETsの利用を提唱した「Privacy-Enhancing Technologies: The Path to Anonymity⁽³⁶⁾」という1995年に公表された報告書においてである。

プライバシー保護のための対策を講じることは、プライバシー保護とセキュリティ対策の関係に見られるように、トレードオフの問題が発生する。例えば、セキュリティ対策を講じるために監視カメラを用いると、結果的に監視対象になる人物のプライバシーが制限される問題などが典型である。この問題を解消するため、④ゼロサム (一方当事者にはプラスであるが他方の当事者にはマイナスのため、結果的にゼロになってしまうこと) ではなくポジティブサム (両者ともプラスになること) という原則を示している。

これらの取組みは、事前に計画されるものであるが、それを計画的かつ継続して実施することが重要であることから、⑤個人情報の取扱い (ライフサイクル) 全般にわたって適切な保護がなされる必要がある。さらに、どのような取組みがなされているのか、⑥可視化と透明性を確保することで利用者の信頼を確保するとともに、取組みの状況を明らかにすることで社会的信用を獲得することができる。

以上の取組みは、個人情報を取扱う側の理屈ではなく、個人 (本人) の視点から適切なプライバシー保護のあり方を考えることが必要となるため、⑦個人のプライバシー尊重に基づいて実施されるべきという理念が最後の原則である。

6. 事前評価の必要性

個人情報の取扱いに関して、個人のプライバシーに与える影響やリスクを事前に評価する手法として、「プライバシー影響評価」(PIA: Privacy Impact Assessment)という手法がある。この手法は、行政情報システムにおける個人情報の適正な取扱いを確保し、個人のプライバシーを保護するために最適な方策を講じるために実施するための評価手法として考案されたものである。

その目的は、①プライバシーへの影響を最低限にするための「方策(制度面での対応)」の検討、②プライバシー・個人情報保護のために実施可能な「対策(技術的な対応)」の検討、③情報システムの事後的な大幅仕様変更を防ぐことで不要な支出を防止することである。

社会保障・税の一体改革においては、社会保障・税番号(マイナンバー)の導入を目指すマイナンバー法案において、「特定個人情報保護評価」として我が国で最初のPIAが実施される予定である。なお、プライバシー影響評価の詳細については、拙著⁽³⁷⁾を参照されたい。

PIAは、行政機関が構築する情報システムを対象に事前評価を実施することを念頭に置いた手法である。したがって、民間事業者による情報の取扱いに当該手法が直接適用されることは前提としていない。しかし、行政機関が保有する情報に匹敵またはそれ以上の情報を保有し利用している事業者が存在することは周知の事実⁽³⁸⁾である。そのため、民間事業者においても、情報システムを構築するにあたって、個人のプライバシーに及ぼす影響を事前に評価する意義は大きいといえる。

なお、特定個人情報保護評価においては、マイナンバーを取り扱う国の行政機関等や地方自治体が実施の義務を負うことはもとより、情報提供ネットワーク(情報連携基盤)を利用してマイナンバーを取り扱う民間事業者もその対象になる。一方、情報提供ネットワークを利用してマイナンバーを取り扱わない一般の事業者(情報連携基盤を用いてマイナンバーの提供や照会を行わない事業者)については、マイナンバーを取り扱う場合であってもその取扱いについては法令の範囲でその取扱いが定められているため、そのような事業者まで特定個人情報保護評価の対象にする必要はないと考えられる。

7. マネジメントシステム活用のあり方

個人情報の適正な取扱いと保護を行う上で、マネジメントシステムを活用し組織的・体系的・継続的な取組みを行う方法がある⁽³⁹⁾。個人情報保護に関するマネジメントシステムは、JIS Q 15001:2006「個人情報保護マネジメントシステム—要求事項⁽⁴⁰⁾」が主な規格となっている。

マネジメントシステムは、PDCAサイクルによって、継続的な改善を行うことでスパイラルアップを図ることを目指している。その過程において、教育の実施や日々の点検により、

個人情報の取扱いに係る各種記録や手続きの実施状況を確認することで、最終的な監査において不適合とされた点を見直すことで、更なる発展的な対応が可能となるものである。しかし、マネジメントシステム構築にあたっての事前の膨大な労力に対し、マネジメントシステムを動かし実際に個人情報の取扱いが行われる段階に至って、当初の目的が逆に業務の支障になったり、過度な負担と受け止められることもある。

その結果、当初の目的とは異なり、本来目指すべき個人情報の適正な取扱いと保護が行われず、マネジメントシステムの存在意義が低下してしまい、スパイラルアップどころかスパイラルダウンによって本来目指すべき目的が達成できないだけでなく、逆にリスクを増大させてしまう恐れすらある。そのように、まるで絵に描いた餅だけが存在し続け、形式的、形骸的な取組みを続けることほど、無意味で、無駄な労力を費やすことは全く不幸である。

そこで、新たに個人情報保護への取組みを開始するときに限らず、既にマネジメントシステムを構築するなどして個人情報保護への取組みを行っている組織においても、前述の「プライバシーバイデザイン」に基づく取組みを行うことや、改めて、現実に即した実効性ある個人情報保護への取組みを再考することが必要な場合があることを認識することが求められている。

その他、新たな事業において、行政機関による許可や認可等が必要なのかを事前に確認する制度として、「法令適用事前確認手続(ノーアクションレター)⁽⁴¹⁾」という制度がある。法令遵守の目的を達成する上で、当該制度を活用することは有用であろう。

8. いわゆるビッグデータの取扱い

情報の取扱いを巡る環境変化として、近時議論がなされる機会が増えているものにビッグデータの取扱いを巡る問題がある。ビッグデータという用語については、「特定のデータがデータベース等を用いて体系的に構成されているのではなく、大量の情報が散在したままの状態の非構造化データのことをいう⁽⁴²⁾」と筆者なりの定義を試みたが、当該用語はあくまで「クリシェ(中身がない用語)」である。

ビッグデータの取扱いを通じて、大量かつ貴重な情報の取扱いに係る法的責任を自覚し、ビッグデータ時代における法令遵守のあり方を検討することが喫緊の課題となっていることは事実である。しかし、いわゆるビッグデータの取扱いに伴う法的課題については、従来から議論されてきた問題から大きくかけ離れた新たな課題はないと思われる。

真の問題は、「ユニークな(独自の、独特な)」取組みが、気がついたら別の意味の「ユニークな(風変わりな)」に変わってしまったことが多々あることである。これは、ビッグデータの取扱いを巡る対応や検討にも同様の懸念があることに留意しなければならない点である。ビッグデータ活用といながら法令に違反するような取扱いを行ったり、的外れなコンプライアンスに労力を費やすことの愚かさを指摘せざる

を得ない状況も散見される。情報技術の急激な変化といった外部環境の変化や、社会的変化への対応に遅れまいという焦りによって、それらに大きく影響され振り回される結果、コンプライアンスやマネジメントの面で空洞化が生じているのではないと思われる事例も見受けられる。

重箱の隅をつつくような法解釈をしながら、本人同意のあり方、機微情報の取扱い、プライバシーポリシーの意味、第三者機関の不存在など、国際標準(プライバシーコミッショナー会議における認定基準等)からはかけ離れた非常識な対応がまかり通っている現状を今後も放置し続けると、法令を遵守しない企業が跋扈し、無意味なコンプライアンスに労力を費やす企業の競争力が落ち込む恐れがあることを、皮肉にもビッグデータ活用を巡る議論によって認識しなければならぬ状況になりつつある。

9. ライフログ活用サービスにおける 配慮原則

ビッグデータ活用の典型例は、大量に取得されるデータを行動ターゲティング広告等に活用する取組みが挙げられる。

現行の法令において定められている義務を遵守することはもとより、適正な情報の取扱責任を果たすためには、自主的な規制等も確認しておくことが必要である。

総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会(第二次提言案)」(平成22年5月)では、ライフログ活用サービスに関する検討がなされ、我が国のライフログ活用サービスの現状、諸外国の対応状況、我が国において懸念される法的問題、より信頼されるサービスに向けて(配慮原則の提言)、ディープパケットインスペクション技術(DPI)を活用した行動ターゲティング広告について検討がなされた⁽⁴³⁾。なお、「ライフログ」という用語は、法学の分野では日本国内においてのみ利用されているといっても過言ではなく、国外では1件のローレビュー論文⁽⁴⁴⁾が当該用語を用いて論じているにすぎない。したがって、ライフログという用語を用いてプライバシー関係の国際会議等で議論するにあたっては、国外における意味との違いに留意する必要がある⁽⁴⁵⁾。

我が国のライフログ活用サービスの現状については、ライフログ活用の二つの方向性として、①利用者の興味・し好にマッチした情報を提供するサービス(行動ターゲティング広告、行動支援型サービス)及び②統計情報を提供するサービスについて、我が国において懸念される法的問題としては、個人情報保護法との関係について主に検討がなされている。具体的には、個人情報への該当性と行動ターゲティング広告等への適用、並びに、特定の個人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にあたるかについて検討がなされている。

更に、プライバシー等との関係について、①プライバシー侵害の有無・程度及び②利用者の不安感等について検討がなされている。以上の検討を踏まえて、より信頼されるサービ

表2 ライフログ活用サービスにおける配慮原則 (総務省ライフログ研究会) 総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会第二次提言」(平成22年5月26日) <http://www.soumu.go.jp/menu_news/s-news/02kiban08_02000041.html>.

① 広報、普及・啓発活動の推進
対象事業者その他の関係者は、利用者のリテラシーの向上や不安感や不快感の払拭に資するべく、対象情報を活用したサービスの仕組みや、本配慮原則に基づく取組について、広報その他の啓発活動に努めるものとする。
② 透明性の確保
対象事業者その他の関係者は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知り得る状態に置く(以下「通知等」という。)よう努めるものとする。通知等に当たっては、利用者が容易に認識かつ理解できるものとするよう努めるものとする。
③ 利用者関与の機会の確保
対象事業者は、その事業の特性に応じ、対象情報の取得停止や利用停止等の利用者関与の手段を提供するよう努めるものとする。
④ 適正な手段による取得の確保
対象事業者は、対象情報を適正な手段により取得するよう努めるものとする。
⑤ 適切な安全管理の確保
対象事業者は、その取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要かつ適切な措置を講じるよう努めるものとする。
⑥ 苦情・質問への対応体制の確保
対象事業者は、対象情報の取扱いに関する苦情・質問への適切かつ迅速な対応に努めるものとする。

スに向けて(配慮原則の提言)が示されている。

配慮原則の対象について、①対象情報は、配慮原則の対象となる情報は、特定の端末、機器及びブラウザ等(以下「端末等」という。)を識別することができるものとする。対象情報は、個人情報保護法上の個人情報であるか否かを問わない。②対象事業者については、対象となる事業者は、対象情報を事業(ただし、対象情報を蓄積せずに行う事業は除く。)の用に供している者となっている。配慮原則は、表2の六つである。

10. スマートフォンプライバシー イニシアティブ

スマートフォンは、個人情報の取扱いに関して大量の情報の取得ツールであるだけでなく、日常的に携帯するため個人のプライバシーにも直結する情報が取得されている。犯罪や不正利用も問題となっており、スマートフォンに記録されている情報の証拠能力⁽⁴⁵⁾やその取得方法⁽⁴⁶⁾についても議論⁽⁴⁷⁾されるようになってきている。

スマートフォンを介して様々な情報が取扱われているだけでなく、実際にどのような情報の取扱いが行われているのか、利用者が十分に認識できない状況が存在する。また、アプリケーション提供者においても、どのような利用者情報を取得し利用することが現行の法制度の下において適正な情報の取扱いにあたるのか、十分に理解した上で情報を取得している

とはいいい難い状況がある。

そのような状況を踏まえて、総務省に「スマートフォンを
経由した利用者情報の取扱いに関するWG」が設置され、2012
年1月から検討が開始された。検討会においては、スマート
フォンの利用者情報に係る事実関係及び主な論点を精査し、
利用者が少なくとも注意すべき事項を「スマートフォン・プ
ライバシー・ガイド」として取りまとめるとともに、スマー
トフォンの利用者情報の取扱いに関する「スマートフォン利
用者情報取扱指針」が、「スマートフォン・プライバシー・イ
ニシアティブ利用者情報の適正な取扱いとリテラシー向
上による新時代イノベーション」<[http://www.soumu.go.jp/
menu_news/s-news/01kiban08_02000087.html](http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html)>（以下、「SPI」と
いう。）として、2012年8月7日に公表されている。

SPIは、スマートフォンを対象にした指針ではあるが、利
用者情報の適正な取扱いに関し、いわゆるビッグデータの取
扱いにあたって留意すべき事項が詳細に示されている。その
上で、スマートフォンにおける利用者情報の取扱いに関する
課題として以下の事項（表3）についての課題認識及び指針が
示されている。

SPIでは、アプリケーション提供者等の関係事業者等が利
用者情報を適正に取り扱う上で従うことが望ましい具体的
な規範として、「スマートフォン利用者情報取扱指針」（図2）を
提示している。

11. 近時の国際動向

クラウドコンピューティングをはじめとして、データが国
境を越えて流通する状況が常態化しつつある中で、個人情報・
プライバシー保護を巡る問題については、国際的な動向も注
視することが不可欠である。紙幅の関係で近時の国際的な動
向については、OECD、EU、APECにおける動向について若
干紹介するにとどめたい。

表3 スマートフォンにおける利用者情報の取扱いに関する課題
筆者作成（私論）。

(1) スマートフォンにおける利用者情報の適正な取扱いの在り方
① スマートフォンにおける利用者情報の性質・分類 スマートフォン上の利用者情報の適正な取扱いの在り方を 論ずる前提として、スマートフォン上の利用者情報の取扱 いと現行法制度等との関係性を整理
② スマートフォンにおける利用者情報の適正な取扱いの在り方
①の整理を踏まえ、関係事業者等が利用者情報を適正に取り 扱う上で従うことが望ましい具体的な規範について整理
(2) 利用者に対する情報提供・周知等の在り方
スマートフォンの一層の普及が見込まれる中で、広く青少 年から高齢者までの幅広い利用者が安全・安心に利用でき る環境を整備するためには、利用者のリテラシー向上のた めの環境作りの方策について整理
(3) 国際的な連携の推進
スマートフォンにおけるプライバシー問題が諸外国におい ても政策課題となっており、こうした課題の解決には外国事 業者を含む多くの関係事業者の連携が極めて重要になって いることから、国際的な連携の推進の在り方について整理

スマートフォン利用者情報取扱指針の構造

- 利用者情報に係る利用者の不安解消は、一義的に関係事業者の役割と責任で、自主的に行うべき。
- 業界団体未加入のアプリ提供者も含め多様な関係事業者が直接参照できる指針を提示。各業界団体が
業界の実情を踏まえ、追加的事項を盛り込んでガイドラインを作成することも期待される。

- 【総論】 **1 基本原則** → ① 透明性の確保 ④ 適切な安全管理の確保
2 適用対象 ② 利用者関与の機会の確保 ⑤ 苦情・相談への対応体制の確保
3 用語の定義 ③ 適正な手段による取得の確保 ⑥ プライバシー・バイ・デザイン
- 【各論】

1 利用者情報取得者における取組み（アプリ提供者、情報収集モジュール提供者、広告配信事業者）

(1) プライバシー・ポリシーの作成

- ☞ 以下の項目を記載したプライバシーポリシーを、アプリケーションや情報収集モジュールごとに分かりやすく作成する。（簡略版も作成する。）

- （記載項目）
① 情報を取得するアプリ提供者等の氏名又は名称	⑤ 通知・公表又は同意取得の方法、利用者関与の方法*1,2
② 取得される情報の項目	⑥ 外部送信・第三者提供・情報収集モジュールの有無
③ 取得方法	⑦ 問合せ窓口
④ 利用目的の特定・明示	⑧ プライバシーポリシーの変更を行う場合の手続

- *1 同意取得：一部のプライバシー性の高い情報については、原則同意を取得する。（電話帳、位置情報、通信履歴等）
*2 利用者関与：利用者がアプリによる利用者情報の利用や取得の中止を希望する場合に、その方法を記載する。

(2) 適切な安全管理措置

- ・利用者情報の漏洩、滅失、毀損の危険回避の措置
- ・情報収集モジュール提供者に関する特記事項
- ・アプリケーション提供者へ①取得する情報の項目、②利用目的、③第三者提供の有無等について通知する。

2 その他の関係事業者における取組

- (1) 移動体通信事業者・端末提供事業者：アプリ提供者の適切な取扱い支援・啓発活動、連絡通報窓口の整備等を行う
(2) アプリ提供サイト運営事業者、OS提供事業者：同上、OSによる利用許諾がある場合に分かりやすい説明を行う
(3) その他関係する事業者：アプリケーション紹介サイトは有益な情報源となり得る

図2 スマートフォン利用者情報取扱指針 [総務省作成資料。総務省「スマートフォン・プ
ライバシー・イニシアティブ ー利用者情報の適正な取扱いとリテラシー向上による新時代イノベ
ーション」<http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html>]

OECD（経済協力開発機構）は、1980年に「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告（8原則）」を公表したが、30年を経過したためガイドラインの改正に向けた検討を行っている。コンピュータが普及し始めたガイドライン制定当時から、インターネットが利用されるようになった現在に至るまでの個人情報の取扱状況の変化に対応した内容への改正が主たる課題である。

OECDにおける我が国の取組みの一つとして、オンラインにおける青少年保護に関する政策・立案に関する相互理解の促進、及び国際的協力によってインターネットにおける青少年保護を促進する方法の探究が挙げられる。その成果として、「オンラインにおける青少年保護に関する勧告（Council Recommendation on the Protection of Children Online）」が、我が国主導による提案の結果、2012年2月にOECD理事会勧告として採択されている。

EU（欧州連合）は、1995年に、欧州連合加盟国の個人データ保護制度の基本的枠組みを提示し、各国が個人データ保護に関する国内法の整備を行う際に盛り込むことが必要な規定を示した「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」（個人データ保護指令）を採択したが、2012年1月25日に公表されたEUの「個人データ保護規則案」として改正へ向けた検討が行われている。

APEC（アジア太平洋経済協力）は、加盟エコノミーにおける整合性のある個人情報保護への取組みを促進し、情報流通に対する不要な障害を取り除くことを目的として、「APEC プライバシーフレームワーク」（2004年10月29日採択）に基づく、「APEC 越境 プライバシー規則」（APEC Cross-Border Privacy Rules（CBPRs））及び「APEC データ・プライバシー・パスファインダー」プロジェクトを実施している。

以上のとおり、個人情報・プライバシー保護に関する国際的な枠組みは、この1～2年以内にネットワーク社会に対応した新たな内容へと進化しつつある。これらの検討に大きな影響を及ぼしているのが、個人情報・プライバシー保護について専門的知識を有し、国内における法執行のみならず国際的な越境協力を行う各国の「プライバシーコミッショナー」である。

12. 第三者機関の役割

研究開発者が、本稿で述べた個人情報・プライバシーに関する問題に関し、現行の法令においては必ずしも規制・禁止はされておらず違法な情報の取扱いにはあたらないとの判断には至ったものの、不適正な取扱いに該当する可能性がある場合、つまり「グレー」な情報の取扱いについて検討が必要になった場合、誰に問い合わせるとよいのか。

我が国の個人情報保護制度は、各省庁の大臣が個別分野を所管する主務大臣制による法執行体制となっている。そのため、所管分野における個人情報の取扱いが法令の定める義務に違反する場合に、法を執行（報告徴収、勧告、命令）する仕

組みとなっている。つまり、法令に違反した場合に主務大臣が個人情報取扱事業者に報告を求める仕組みはあるものの、法令に違反していない場合に報告を徴収したり、逆に行政から何らかのアドバイスを与える制度にはなっていない。前述の法令適用事前確認手続（ノーアクションレター）にしても、許可・認可等の必要性の有無について行政に問い合わせる仕組みにとどまっている。

そのため、いわゆるグレーゾーンにおける情報の取扱いについては、事業者の自主責任に委ねられており、その結果、グレーの部分リスクと考える事業者は情報の取扱いに消極的な対応を取らざるを得ないため、結果的に、いわゆる過剰反応が生ずる結果となっている。

この問題を解決する切り札として、諸外国において設置されている「プライバシーコミッショナー」が挙げられる。

残念ながら、現時点において我が国にはそれに該当する機関が設置されていない。しかし、社会保障と税の一体改革として、「社会保障・税番号大綱（以下「大綱」という。）」が2011年6月28日にとりまとめられ、国民一人一人に番号を割り当てる「社会保障と税に関わる番号制度（以下「番号制度」という。）」の導入が決定し、番号制度に係る個人情報保護法制の円滑な執行と適切な運用を担保するために、第三者機関の設置が検討されている。

正確な所得等の情報に基づく適切な所得の再分配を実施し、社会保障給付を適切に受ける権利を守るために、「社会保障・税番号（マイナンバー）⁽⁴⁹⁾」を用いて正確な本人特定を行うことが、番号制度の目的である。しかし、番号の利用に伴い、国家による国民の管理、個人情報の追跡・突き合わせ、財産その他の被害等様々な課題が指摘されていることから、監督機関の設置が不可欠と考えられている。

マイナンバーの導入に向けて審議予定の「行政手続における特定の個人を識別するための番号の利用等に関する法律案」（通称：「マイナンバー法案」）では、第三者機関として「個人番号情報保護委員会」が国家行政組織法第3条に基づくいわゆる「三条機関（独立行政委員会）」として明記され、設置等（内閣総理大臣の下に委員会を置く）及び権限、機能（調査、助言、指導等）について定めている。

設置にあたっては、監視機能を実効あらしめるべく、どのように独立性を担保しどのような権限を持つべきかという観点から、責任主体、設置形態、人事（人員構成）、調査権限、規模等の論点について、諸外国の事例も踏まえながら、十分に検討することとされている。

番号法に基づく第三者機関は、あくまで「番号制度に係る個人情報保護法制の円滑な執行と適切な運用を担保」を目的に設置される機関である。

本稿執筆段階では、第三者機関はマイナンバー法案において示されている「個人番号情報保護委員会」の設置（表4）にとどまるが、マイナンバーにとどまらない個人情報保護一般を巡る諸問題にも適切に対応することができる「個人情報保護委員会」の設置が期待される。

表4 第三者機関の設置 「社会保障・税番号大綱」(2011年6月28日).

(1) 内閣総理大臣の下に、番号制度における個人情報の保護等を目的とする委員会(以下「委員会」という.)を置く
(2) 委員会は、次のような業務を行う
ア 行政機関、地方公共団体、関係機関又は「番号」を取り扱う事業者(以下「監督対象機関等」という.)による「番号」に係る個人情報の取扱いの監督
イ 「番号」に係る個人情報の取扱いに関する苦情の処理
ウ 情報連携基盤及びその他の機関と接続する部分の監査
エ 情報保護評価の実施に関する助言及び報告書の承認
オ 番号法に係る適格認証手段の承認
カ 所掌事務に係る国際協力
キ 「番号」に係る個人情報の保護方策並びに番号法に関する普及啓発及び相談の受付

13. 今後のあり方

プライバシー保護のために新たな技術開発を躊躇したり、法令遵守がイノベーションの足かせになることは適切ではない。しかし、新たな技術の利用によって個人の権利利益が侵害されることも防がなければならない。

これを解決するための一つの手法として、プライバシーバイデザインを取り上げた。事後的に、問題が発生してから改善をしたり対応するのではなく、あらかじめ、問題が発生することを予防することの重要性は、高度な情報システムの構築、大規模なデータベースの利用、ビックデータの活用と、情報の取扱いのダイナミズムが増している現状においては、誰しもがその重要性について認識しているといえよう。

現行の制度的課題として、個人情報保護法は個人情報の取扱分野ごとに、各省の主務大臣が法を執行(報告徴収、勧告、命令)する仕組みとなっている。しかし、本稿において言及した諸問題に対応するにあたっては、各省の主務大臣が個々に検討を行うには限界がある事例が増えている。更に、これらのサービスの利用に伴う国際的な個人情報の流通も一層進むものと考えられることから、個人情報・プライバシー保護のための適切かつ統一的な対応を行うことが不可欠となっている。個人情報・プライバシー保護を巡る環境変化に適宜柔軟に対応できる仕組みを整備するとともに、国際的な共助・越境協力を行う上で必要な体制の構築が求められる。

文 献

- (1) J. M. Blanke, ““Robust notice” and “Informed consent:” the keys to successful spyware legislation,” *Colum. Sci. & Tech. L. Rev.*, vol.7, p.2, 2006.
- (2) S. L. McLaughlin, “Controlling smart-phone abuse: the fair labor standards act’s definition of “Work” in non-exempt employee claims for overtime,” *Kan. L. Rev.*, vol.58, p.737, 2010.
- (3) 辻井重男, “情報社会のセキュリティと倫理の課題,” *IEICE Fundamentals Review*, vol.1, no.3, pp.10-26, 2007.
- (4) 新保史生, “監視・追跡技術の利用と公法的側面における課題,” プライバシー・個人情報保護の新課題, 堀部政男(編), pp. 193-234, 商事法務, 東京, 2010.
- (5) L. Ellison, “Soft surveillance hard consent,” Ian Kerr, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, p.8, Oxford Univ Pr, 2009.

- (6) 石井夏生利, 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, 東京, 2008.
- (7) D. Lyon, *Surveillance Society : Monitoring Everyday Life*, Open University Press, 2001.
- (8) M.-A. Poirier, “Employer monitoring of the corporate E-mail system: how much privacy can employees reasonably expect?,” *U.T. Fac. L. Rev.*, vol.60, p.85, 2002.
- (9) C. J. Bennett, “Workplace monitoring: cyber-snooping, and cookies: creating standards for watching or not watching: information policy and information privacy: international arenas of governance,” *U. Ill. J.L. Tech. & Pol’y*, vol.2002, p.385, 2002.
- (10) M. C. Keck, Cookies, “The constitution, and the common law: a framework for the right of privacy on the internet,” *Alb. L.J. Sci. & Tech.*, vol.13, p.83, 2002.
- (11) D. M. Antonialli, “Watch your virtual steps: an empirical study of the use of online tracking technologies in different regulatory regimes,” *Stan. J.C.R. & C.L.*, vol.8, p.323, 2012.
- (12) A. D. S.-Raham, “Carrier IQ, pre-transit keystroke logging, and the federal wiretap act,” *N.C. J.L. & Tech.*, vol.13, p.417, 2012.
- (13) A. Candeub and D. J. McCartney, “Network transparency: aeeing the neutral network,” *Nw. J. Tech. & Intell. Prop.*, vol.8, p.228, 2010.
- (14) P. Ohm, “The rise and fall of invasive ISP surveillance,” *U. Ill. L. Rev.*, vol.2009, p.1417, 2009.
- (15) J. Weinberg, “Governments, privatization, and “Privatization” : ICANN and the GAC,” *Mich. Telecomm. Tech. L. Rev.*, vol.18, p.189, 2011.
- (16) 新保史生, “個人情報保護法に基づくバイオメトリクスの利用,” 情報メディア研究, vol.4, no.1, pp.62-63, 2006.
- (17) R. D. Covey, “Pervasive surveillance and the future of the fourth amendment,” *Miss. L.J.*, vol. 80, p.1289, 2011.
- (18) B. R. Stancombe, “Fed up with being felt up: The complicated relationship between the fourth amendment and TSA’s “Body Scanners” and “Pat-Downs”,” *Cumb. L. Rev.*, vol.42, p.181, 2012.
- (19) J. Le. Vine, “Over-exposed? TSA scanners and the fourth amendment right to privacy,” *J. Tech. L. & Pol’y*, vol.16, p.175, 2011.
- (20) R. Murphy, “Routine body scanning in airports: a fourth amendment analysis focused on health Effects,” *Hastings Const. L.Q.*, vol.39, p.915, 2012.
- (21) N. J. King, S. Pillay, and G. A. Lasprogata, “Workplace privacy and discrimination issues related to genetic data: a comparative law study of the european union and the united states,” *Am. Bus. L.J.*, vol.43, p.79, 2006.
- (22) 新保史生, “ネット検索サービスとプライバシー,” 法とコンピュータ no.28, pp.71-78, 2010.
- (23) クラウド・コンピューティングの法律, 岡村久道(編), 民事法研究会, 東京, 2012.
- (24) A. Lavoie, “The online zoom lens: why internet street-level mapping technologies demand reconsideration of the modern-day tort notion of “Public Privacy,” *Ga. L. Rev.*, vol.43, p.575, 2009.
- (25) A. A. Otterberg, “GPS tracking technology: the case for revisiting knots and shifting the supreme court’s theory of the public space under the fourth amendment,” *B.C. L. Rev.*, vol.46, p.661, 2005.
- (26) A. N. Person, “Behavioral advertisement regulation: how the negative perception of deep packet inspection technology may be limiting the online experience,” *Fed. Comm. L.J.*, vol.62, p.435, 2010. R. T. G. Collins, “NOTE: the privacy implications of deep packet inspection technology: why the next wave in online advertising shouldn’t rock the self-regulatory boat,” *Ga. L. Rev.*, vol.44, p.545, 2010.
- (27) D. Lyon, “National IDs in a global world: surveillance, security, and citizenship,” *Case W. Res. J. Int’l L.*, vol.42, p.607, 2010.
- (28) H. R. Frisby, Jr. and J. P. Trotta, “The smart grid: the complexities and importance of data privacy and security,” *CommLaw Conspectus*, vol.19, p.297, 2011. A. Schira, “Protecting progress and privacy: the challenges of smart grid implementation,” *ISJLP*, vol.6, p.629, 2011.
- (29) E. Union, “EU study on the legal analysis of a single market for the Information society, new rules for a new age?,” Nov. 2009, http://ec.europa.eu/information_society/newsroom/cf/document.

cfm?action=display&doc_id=833(Last accessed 2012/09/27).

- (30) W. L. Prosser, J. W. Wade, and V. E. Schwartz, Cases and Materials On Torts, Foundation Pr, 1982.
 - (31) 藤原静雄, 個人情報保護法制研究会, 個人情報保護法の解説改訂版, 園部逸夫(編), ぎょうせい, 東京, 2005. 岡村久道, 個人情報保護法新訂版, 商事法務, 東京, 2009.
 - (32) 新保史生, プライバシーの権利, 憲法入門, 山本順一(編), p.50, 勉誠出版, 東京, 2003.
 - (33) 山田卓生, 私事と自己決定, 日本評論社, 東京, 1987.
 - (34) L. H. Tribe, American Constitutional Law, 2nd ed., Foundation Pr, 1988.
 - (35) 最判平成12年2月29日. なお, 医療における個人の自己決定をめぐる憲法問題については, 竹中勲, 人権としての「自己決定権」, ジュリスト884号180頁を参照. また, 「エホバの証人」信者による信仰上の理由に基づく輸血拒否の問題については, 仮処分が申請された事案があるが, (大分地決昭和60年12月2日判時1180号113頁・判タ570号30頁) 被保全権利について疎明がないとして仮処分申請は却下されている.
 - (36) Information and Privacy Commissioner/Ontario Canada & Registratiekamer (Netherlands), Privacy-Enhancing Technologies: The Path to Anonymity, 1995, <http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf> (Last accessed 2012/09/27).
 - (37) 瀬戸洋一, 六川浩明, 新保史生, 村上康二郎, 伊藤洋昭, プライバシー影響評価PIAと個人情報保護, 中央経済社, 東京, 2010.
 - (38) E. A. Brotherton, "Big brother gets a makeover: behavioral targeting and the third-party doctrine," Emory L.J., vol.61, p.555, 2012.
 - (39) 鈴木正朝, 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, 東京, 2004.
 - (40) 堀部政男, 鈴木正朝, 齋藤雄一, 新保史生, 太田克良, "個人情報保護マネジメントシステム要求事項の解説—JIS Q 15001:2006," 日本規格協会, 2006.
 - (41) 電子政府の総合窓口, 各府省の法令適用事前確認手続(ノーアクションレター) 情報, http://www.e-gov.go.jp/link/no_action_letter.html.
 - (42) 新保史生, "クリシェとしてのビッグ・データ," 情処学・電化知的財産・社会基盤(EIP) 研報, vol.2012-EIP-55, no.7, pp.1-6, 2012.
 - (43) 新保史生, "ライフログの定義と法的責任-個人の行動履歴を営利目的で利用することの妥当性-, 情報管理, vol. 53, no.6, pp.295-310, 2010.
 - (44) A. L. Allen, "Dredging up the past: Lifelogging, memory, and surveillance," U. Chi. L. Rev., vol.75, p.47, 2008.
 - (45) J. A. Engel, "Doctrinal collapse: smart phones cause courts to reconsider fourth amendment searches of electronic devices," U. Mem. L. Rev., vol.41, p.233, 2010.
 - (46) D. Zamani, "There's an amendment for that: a comprehensive application of fourth amendment jurisprudence to smart phones," Hastings Const. L.Q., vol.38, p.169, 2010.
 - (47) C. Lee, "The future of "Reasonableness" analysis: when is a search or seizure justified? reasonableness with teeth: the future of fourth amendment reasonableness analysis," Miss. L.J., vol.81, p.1133, 2012.
 - (48) 新保史生, "社会保障・税に関わる番号制度の導入とプライバシー," Nextcom, no.8, pp.4-13, 2011.
- (SITE研究会提案, 平成24年9月18日受付, 10月30日最終受付)

新保史生 (正員)

平6法政大・経卒. 平11駒澤大大学院法学研究科博士課程了. 同年, 国際通信経済研究所研究員, 平13日本情報処理開発協会研究員, 平14筑波大図書館情報学系助教授等を経て, 現在, 慶大・総合政策・准教授. 専門は憲法, 情報法. 博士(法学). 平15第1回ドコモ・モバイル・サイエンス賞, 平15第18回電気通信普及財団賞テレコム社会科学賞各受賞. 憲法学会理事, 情報通信学会監事, 法とコンピュータ学会理事, 経済協力開発機構(OECD)情報セキュリティ・プライバシー部会(WPISP)副議長.