2021.5.24

成立したデジタル監視法の問題点と今後の課題
総理大臣をトップとする警察監視国家を現実のものとしないために

海渡雄一
（デジタル監視法案に反対する法律家ネットワーク）

内容

第１ 成立したデジタル監視法の問題点 1
第２ 進展する世界的な監視社会化とプライバシー・民主主義の危機 3
第３ 日本の監視社会化の現段階とデジタル庁のインパクト 8
第４ 個人情報保護確立のための今後の課題 11

第１ 成立したデジタル監視法の問題点

１ 法は成立したが・・・

5月 12 日、参議院本会議において、デジタル改革関連6法案（デジタル監視法案）が、自民党、公明党、維新の会、国民民主党の賛成多数により可決・成立した。デジタル監視法案は、そもそも1000 頁を超える 64 本の膨大な束ね法案であるが、2 月 9 日に国会に提出されるまで、その内容は明らかにされなかった。衆・参両院の審議時間は、あわせて50数時間に過ぎなかった。

私たち、デジタル監視法案に反対する法律家ネットワークは、2月の法案国会提出後に結成され、コロナ禍の下で市民集会などの開催が極めて困難な中で、記者会見やオンラインセミナーなどを繰り返し、法案の危険性を市民に伝える努力を続けてきた。法は成立してしまったが、悪法が濫用されないように封じ込めるためにも、私たちの活動は継続しなければならない。

２ プライバシー権は民主主義の基礎

人は監視されていると感じると、自らの価値観や信念に基づいて自律的に判断し、自由に行動して情報を収集し、表現することが困難になる。プライバシー権は、人格的自律を実現し、表現の自由を行使する不可欠な前提条件であり、立憲民主主義の基礎となっている人権である。

デジタル化を推進するためには、プライバシー権の保障を徹底し、自己情報コントロール権を確立し、個人情報の取得、保有、利用、提供、廃棄のすべてに情報主

体である個人の同意を要するとの原則を徹底することが必要である。

３　個人情報の保護が後退する危険性がある

今回成立したデジタル監視法は、情報コントロール権を明記せず、個人情報保護を後退させ、国家による市民監視を強めるものである。

データを取り扱う際に共通仕様化を進めることにより、国の諸機関や地方自治体からデジタル庁に集積された膨大な個人情報が、権利主体の同意なく、企業や外国政府を含む第三者に提供され、目的外に使用される危険性がある。

我々が特に危惧するのは、警察がデジタル庁・内閣情報調査室を経由して、内閣総理大臣としての権限で各省庁・自治体などが保管する情報にパソコンの操作だけでアクセスすることができ、自由に個人情報を取り出せる仕組みができるのではないかということだ。

改正個人情報保護法６９条（利用及び提供の制限）の規定によれば、必要性、相当性があれば、個人の同意なく情報の利活用・第三者提供が可能である。政府は、この条文は改正前と同じであるから、我々の危惧は杞憂であると答弁する。しかし、相当性、必要性という要件は極めてあいまいであり、濫用を防ぐためこの要件をさらに限定しようとした野党修正案に政府は応じなかった。

政府・警察による違法な個人情報の収集・保有、プロファイリングや利用などの怖れはないと、政府は答弁した。しかし、これまでも、内閣情報調査室が文科事務次官であった前川喜平さんや望月衣塑子記者らの行動を監視していたことが明らかになっている。

４　地方自治体による個人情報保護の為の取り組みを後退させてはならない

デジタル監視法は、これまでの分権的な個人情報保護システムの在り方を破壊しようとしている。地方自治体において、住民との合意のもとで構築されてきた独自の個人情報保護の在り方を破壊し、各地で構築されてきた先進的な個人情報保護制度の構築を後退させるものになりかねない。

政府は、自治体における独自の取り組みは否定しないとしている。しかし、自治体の独自の規制を維持するための財政的な裏付けも示されていない。

５　デジタル庁は独裁機関化するかもしれない

デジタル庁は内閣府ではなく、内閣に置かれ、トップは総理大臣である。そして、デジタル大臣は、特に必要があると認めるときは、関係行政機関の長に対し、勧告することができ、行政機関は、当該勧告を十分に尊重しなければならないとされている。これは時限組織である復興庁にしかなかった規定であり、全省庁の中で抜きんでた権限が与えられている。デジタル庁が独裁機関化する危険性は国会審

議でも払しょくされなかった。
　しかし、最初からこのような組織が構想されていたわけではない。昨年 10 月 1 日の朝日新聞記事によれば、「首相のかけ声に見合う推進力をどう与えるかも調整中だ。関係者によると、デジタル庁の位置づけは①復興庁のような内閣直轄②内閣官房③内閣府④内閣官房に司令塔部分、内閣府にシステム構築部分を並立、の 4 案を検討しているという。首相が影響力を発揮し省庁を抑えやすい点で、平井氏らは①を想定するが、組織のトップを大臣格とするか、恒久的か時限的か、予算や事業を担う範囲など組織立ち上げにあたっての論点は多い」（2020 年 10 月 1 日朝日新聞記事「首相の目玉「デジタル庁」の準備室発足 調整事項は山積」より）。とされていた。トップを役人出身の長官にするか、大臣を置くどうかすらも議論されていたのである。
　また、政府答弁によれば、デジタル庁は、発足時は 500 人程度で、非常勤職員が 128 人、その多くは民間企業からの出向だとされる。しかも、庁内には、局も課も置かれないアジャイル型組織とされる。必要に応じて活動内容を迅速に変えていくことができるとされるが、行政組織としてきわめて特殊で不透明な組織構成だ。構成員がトップと直接的につながるアジャイル型組織は、内閣総理大臣によるデジタル情報の国家独占管理体制につながる危険性については、国会審議によっても払拭されなかった。
　また、このような体制で、本当に情報の漏洩が防げるのか、行政と巨大 IT 企業の癒着によって行政が歪められるおそれはないのか、国会審議によっても多くの疑問が解消されたとは到底言えない。
　デジタル庁を独裁機関化させないためには、金融庁や消費者庁などと同様に、内閣ではなく内閣府（の外局）に置き、デジタル庁の長は内閣総理大臣ではなく特命担当大臣であるデジタル大臣とし、デジタル大臣の勧告についての尊重義務の規定はなくすよう、改正を求めていく必要がある。

第 2 進展する世界的な監視社会化とプライバシー・民主主義の危機

1 一国の全国民の個人情報が流出する ！

　世界的な IT 化、監視社会化の流れは、趨勢であり、日本も乗り遅れないようにという論者もおられた。
　しかし、そんなに単純な問題だろうか。最近こんなニュースも報じられている。日経新聞の 9 月 18 日の報道だ。
　「【サンパウロ＝外山尚之】南米のエクアドル政府は 16 日、国民ほぼ全員を含む約 2000 万人分の個人情報が海外に流出したと明らかにした。名前や個人識別番号、銀行口座残高を含む。同国の IT 企業ノバエストラットがセキュリティーの不

十分なサーバーに情報を保管していたことが原因のようだ。実害が出ているかどうかは不明だ。」
「米国にある同社のサーバーに残されていた計 18 ギガバイトのデータは 2000 万人分の個人情報を含む。エクアドルの人口である約 1660 万人を上回るため、死者の情報も含まれているとみられている。」
「vpn メンターは「悪意のある集団が銀行口座などにアクセスするために十分なデータが流出した」と警告している。
エクアドルのモレノ大統領は 16 日、教育・スポーツ相と通信・情報社会相を配置し、事態収束に向けて取り組むと発表した。近日中に、個人情報の保護に関する法律を国会に送る。情報を流出させたノバエストラットの責任者に対し、許可なく個人情報を扱った疑いで当局が捜査を始めた。」
2000万人分の個人情報がわずか 18 ギガバイトという点に驚く。日本国民全体でも 100 ギガバイトもあれば、十分だろう。それが全部流出することだって、ありえないことだろうか。

2 人間を破滅に追い込むこともできるネット監視技術

世界的に監視社会の現状を俯瞰すると、アメリカの NSA が築いたプリズム、スパイのグーグルと呼ばれる XkeyScore のシステムが存在している。
スノーデン氏の告発によれば、NSAは、インターネット時代に即応し、プリズムと呼ばれるデジタル情報の世界的監視システムを構築し、SNSやクラウド・サービス、あるいはインターネットの接続業者など大手のIT企業9社のサーバーから直接網羅的にデータを収集していたという。この9社とは、Microsoft、米 Yahoo、Google、Facebook、AOL、Skype、YouTube、Apple、Paltalk であり、NSAはこれらの会社の保有するサーバーなどに自由にアクセスすることができ、フェイスブックのチャットやグーグルの検索履歴、ヤフーメールなども傍受できたという。すべてのプライバシーを知るということは、その人物の経済的な弱点、秘密の異性関係、過去の前歴などをすべて知ることができる。そして、その弱点を暴くと脅して言うことを聞かせることもできる。
NSAの傍受システムにはプリズム以外にアップストリームによる傍受として、光ファイバーケーブルの情報を収集するシステムとCNEの3種類がある。CNEは対象ユーザーのパソコンをマルウェアに感染させ、すべてのキーストロークや閲覧画面を監視できる。NSAは全世界の5－10万台のパソコンをマルウェアに感染させることに成功しているという。
さらに、7月7日付ワシントンポスト紙によると、FBIは捜査のために、運転免許証のデータベースにある顔写真を無断で使っていたという。犯罪歴のない運転免許保持者の写真も、本人に何も知らせないで、勝手に使われていた。顔認証カメ

ラと連動すれば、監視対象の人物がどこにいるかを明らかにすることもできるのだ。
　アメリカのネット監視技術は、アメリカ政府によるテロ対策の現場で用いられ、多くの個人を破滅のふちに追い込んできた。

3　民主主義の崩壊を招くビッグデータの売買
　フェイスブックの集めていた個人データの蓄積が、重大な選挙の結果に影響を与えた事件が、ケンブリッジ・アナリティカ事件である。
　イギリスの EU 離脱をめぐる国民投票で、選挙キャンペーンを行う会社が、約 8000 万人分のフェイスブックの個人データを買い受けた。僅差が予測されていたが、選挙結果は、イギリスの EU 離脱という結論となった。その背後では、この選挙コンサルタント会社が、個人の属性に即応したターゲット広告によって投票行動をコントロールしていた。
　この件では、イギリスの情報コミッショナーが 2018 年 3 月にケンブリッジ・アナリティカ社の家宅捜索を行い、データサーバーを押収した。このデータはケンブリッジ・アナリティカ社の親会社である SCLE 社がフェイスブック社に 27 万ドルを支払って入手していたことが判明している。利用者の SNS 上の行動から、個人をプロファイリングし、ターゲット広告を行うことによって選挙結果すら左右できることがあきらかになったのである。

4　究極的監視社会となった中国
　他方で、中国は監視カメラとネット監視、スコア制度によって、急速に監視社会システムを構築し、これを発展途上国に売り込み始めている。中国全土に設置された監視カメラはすでに二億台、瞬く間に六億台に達するだろうと言われている。8 月 24 日付の西日本新聞の報道（北京発川原田健雄とクレジットされている）によると、「世界 120 都市の防犯・監視カメラの設置状況について英国の調査会社コンパリテックが調べたところ、住民千人当たりのカメラ設置台数（設置率）が多い上位 10 都市のうち 8 都市を中国が占めた。」という。これらの監視カメラは顔認証システムと連動している。
　米フォーリン・ポリシー誌 2019 年 6 月 24 日号に掲載された「ビッグ・ブラザーがベオグラードに来た」という記事によれば、2014 年にベオグラードで子供のひき逃げ死亡事故を起こした犯人が、中国に逃亡し、セルビア当局が、中国に犯人の顔写真を送った。その後 3 日間で、中国国内に潜伏していたこのひき逃げ犯人を検挙したというのである。
https://foreignpolicy.com/…/big-brother-comes-to…/

この高い捜査効率に驚いたセルビア政府は、中国のファーウェイ社と契約し、今後二年間の間に、ベオグラード市内の 800 か所に 1000 台の高性能監視カメラを設置する計画を公表した。中国製の AI 監視システムを買うことに決めた国は、ニューズウィーク誌（2019 年 4 月 24 日）の調べによれば、すでに 54 か国に達しているという。

アメリカの世界的な監視システムから排除されている国々は急速に中国製の監視社会の導入に動いているように見える。こちらの方が、様子がよくわからず、その規制もより困難である。

スマホの 5G 技術をめぐる米中の覇権争いが世界中で起きている。

この争いは、先端 IT 技術をめぐる経済的な競争としての側面を持っているが、それだけでなく、世界的なデジタル監視システムの覇権をめぐる争いでもあるといえる。

中国ではウィグルやチベットの民族的少数派、労働組合活動家とこれを支援する学生たちなど政府の価値観と異なる思想を持つものは、徹底してマークされ、社会から排除されている。

しかし、他方で、大多数の国民には、高いスコアをとれば、金利も下がり、ビザなども優遇される。顔認証決済で、手ぶらで何も持たなくても買い物ができるシステムとして歓迎されているのだという。

5　香港の人権と民主主義が中国型監視社会によって圧殺されようとしている

香港で一国二制度を守ろうとする市民は、明らかに中国政府から監視対象とされている。香港行政長官は 2019 年 10 月4日緊急状況規則条例を発動し、立法院の手続を省略して覆面禁止法を制定した。デモや集会で覆面を禁じ、違反者には最高1年間の禁錮刑などを科す。監視カメラによる監視から逃れることが犯罪化された。これは国家緊急権による自由の圧殺だ。

2020年6月30日，中国政府はその国体を維持する目的で，国家安全維持法を制定・公布した。そして、同法違反を理由に，デモ参加者，著名活動家，報道機関経営者などが逮捕されている。報道関係者に対する有罪判決も出されている。2021年3月24日，当局は，著名な活動家が同法違反で起訴された。

同法第4条は自由権規約を含む各種国際人権規約は香港にも適用されると規定する。そこで，この法律を国際人権基準の観点から検討すると，まず明確な構成要件が定められていない。国家分裂罪（第3章第1節）については，香港の独立を主張することが犯罪化されるおそれがある。国家政権転覆罪（第3章第2節）については，中国政府・香港の行政当局を批判する表現そのものが犯罪化されるおそれがある。外国または域外勢力と結託して国家の安全を害する罪（第3章第4節）

については，香港の民主勢力が欧米や日本などに支援を求める行為が犯罪化されるおそれがある。

また，審理手続きについても，重大な疑問がある。第44条は，行政庁長官が，事件を処理するため，数名の裁判官を指名し審理に当たらせるものとし，指定された裁判官が，その任期中に国家の安全を害する発言をし，又は国家の安全を害するような行為をしたときは，指定リストから除名されると定めている。このような手続きは，公正な裁判を受ける権利を保障している自由権規約第14条に違反している。さらに，第42条は，国安法違反で起訴された場合，保釈について，被疑者が国家の安全を害する行為を継続しないと信じるに足る十分な理由がある場合でなければ，保釈されないと規定されている。このような制限は，自由権規約第9条第3項後段に反するものである。

イギリス型の民主主義と司法システムが機能していた香港が逃亡犯条例と国家安全法によって、中国の監視システムに呑み込まれようとしている。香港市民の絶望的な闘いは、世界的な監視社会との戦いの最前線となっている。

6 プライバシー権によるネットの規制を求めるヨーロッパ

米中が監視社会における覇者を争う中で、EU は GDPR という規則によって、監視社会化を個人の尊厳、プライバシーによって法的に規制しようとしている。GDPR とは「General Data Protection Regulation」の略である。「一般データ保護規則」と訳される。EU で 1995 年から EU データ保護指令が有効であり、各国はこの指令を国内法化する義務を負っていた。しかし、GDPR は、規則であり、各国の国内法化を待たず、効力を持つ。GDPR は、2018 年 5 月 25 日から施行されている。

GDPR における個人情報の処理については、IP アドレスや Cookie のようなオンライン識別子も個人情報とみなされることとなった。企業は個人情報を取得する場合、自らの身元や連絡先、処理の目的、第三者提供の有無、保管期間などについてユーザーに明確に告知し、同意を得なければならないこととなった。勝手に Cookie などの方法で個人情報を集めてはならないのである。大量の個人情報を扱う企業はデータ保護オフィサーを任命しなければならないこととなった。個人情報を使用する目的を達成するために必要な期間以上に個人情報を保持してはならないことも定められた。そして、GDPR に違反したときには厳しい罰則が科されることとなった。最大で企業の全世界年間売上高の 4%以下、あるいは 2000 万ユーロ以下のいずれか高い額の罰金を科すことができることとなった。EU 域内の顧客に対して、ネット上で取引を勧誘するには、世界中のどの地域の企業であっても、この GDPR に準拠することが必要になったのである。

第３　日本の監視社会化の現段階とデジタル庁のインパクト

１　共謀罪の推進勢力が外務省・法務省から官邸に途中で変わった

　2012年に誕生した安倍政権は、まず特定秘密保護法を制定した。これを進めたのは、公安警察出身の官邸官僚である内閣情報官（当時）の北村滋氏であった。共謀罪は、国際的組織犯罪防止条約に基づき創設されるものであると政府から説明されたが、そもそも、この条約はマフィア対策、テロ対策の条約ではない。この条約は、組織犯罪集団への参加又は重大な犯罪の共謀の処罰を求めたものである。2003年に政府は共謀罪法案を国会に提案（必要性はないが、条約批准のためにとの説明）したが、この時点での共謀罪法案の推進勢力は、外務省と法務省であった。2005/6年には国会審議が始まったが、日弁連などの強い反対もあり、法案は廃案になった。民主党政権下では、共謀罪法なしに条約を批准する途も模索された。そして、その後、共謀罪法の制定を目指す推進力となったのも、やはり北村氏であった。

２　制定20年を経過した盗聴法の適用が飛躍的に拡大する危険性がある

　2015年に改正された盗聴法（通信傍受法）が2019年6月1日から全面的に施行された。盗聴法が2000年に制定された際、私たちは大きな反対運動を組織して、これに抵抗した。反対運動の効果もあり、対象犯罪は覚せい剤などの薬物と銃器の取引、組織的殺人、集団密航の4種類の犯罪に限定した。また、傍受が適切に行われることを確保するために、NTTなど通信事業者の常時立ち会いを義務づけることとした。

　このような強い規制により、通信傍受を行った事件数、令状の発布件数は少しずつ増えてきたが、激増するには至っていなかった。

2015年改正では、新たに、9つの犯罪（窃盗、詐欺、殺人、傷害、放火、誘拐、監禁、爆発物、児童ポルノ）盗聴可能犯罪として追加された。この中の窃盗と詐欺は、刑務所に入っている人の数でいえば圧倒的な多数で、犯罪件数では年間100万件を超えている。

　また、手続きも緩和されている。具体的には、通信事業者は令状に示されたすべての通信を録音し、これに暗号をかけて、警察署に送信する。警察官は、警察署内でいつでもこの暗号を解いて、傍受された通信を聞いたり、見たりすることができる。そして、この暗号化の方法を用いれば、外部の事業者の立会なく、都道府県の警察本部や検察庁で居ながらにして直接盗聴できることとなった。このような制度改正により、これまで必要以上の盗聴が規制されていた歯止めが破られ、その実施件数が飛躍的に拡大する危険性がある。なお、盗聴の実態は国会に報告されることから、国会がこれを注視し、野放図な拡大を食い止めることを期待したいが、実際には大きな壁がある。

3　監視カメラと顔認証技術が結び付けば、究極の監視社会が現実のものとなりうる

　西日本新聞（2019/8/24 6:00西日本新聞国際面）の報道によると、「世界120都市の防犯・監視カメラの設置状況について英国の調査会社コンパリテックが調べたところ、住民千人当たりのカメラ設置台数（設置率）が多い上位10都市のうち8都市を中国が占めた。現在約2億台ある中国の監視カメラが2022年までに6億2600万台へ大幅に増加するとの推計も示し、監視社会が進む実態を指摘した。同社の報告書によると、監視カメラの設置率が最も高い都市は中国の重慶で、千人当たり168台に上った。2位は深圳（千人当たり159台）、3位上海（113台）、4位天津（92台）、5位済南（73台）と続いた。6位にロンドン（68台）が入ったが、7位は武漢（60台）、8位広州（52台）、9位北京（39台）と中国の都市が上位をほぼ独占した。10位は米アトランタ（15台）だった。少数民族ウイグル族への抑圧政策の一環として、多数のハイテク街頭カメラによる監視が指摘されるのは、中国新疆ウイグル自治区のウルムチであり、その設置状況は千人当たり12台で14位だった。公表された上位50都市に日本の都市は含まれなかった。」とされている。

4　官邸は官邸ポリスの集めた情報で官僚・政治家を恐怖支配している

　2018年末に「官邸ポリス」と言う題名の本が講談社から出版された。著者は「東京大学法学部卒業、警察庁入庁、その後、退職」とだけ、紹介され、経歴も年齢もわからない。内容は、安倍政権に奉仕する官邸内の警察官僚をはじめとして、外務省、財務省、警視庁、さらには報道機関などの生々しい実態が描かれている。この本は、政権に奉仕し、政権をコントロールさえしようとしている、杉田官房副長官（内閣人事局長を兼務。1997年当時内閣情報調査室長）と北村滋内閣情報官（当時）ら官邸ポリスを告発するために、書かれた内部告発本のようだ。

　2019年6月の毎日新聞のインタビューで、前川喜平元文科事務次官は、『この本が本当だとしたら、現代の特高警察だと思いますよ。私は2016年の9月か10月ごろ、警察庁出身の杉田和博官房副長官から官邸に呼び出され「新宿の出会い系バーというところに行っているそうじゃないか」と言われた。「週刊誌から聞いた話だ」と。それなら週刊誌が私のところに来るはずですが、来ませんでした。…菅さんが総理になれば、もっとひどい警察国家、恐怖政治になるのではないかと懸念しています。…そういえば杉田さんに官邸に呼ばれた時、「〇〇省の〇〇次官にもそういうことがあったよ」と言われたんです。それで「みんな尾行されているのかな」と思った。弱みを握られている人は役人だけではなくて、与野党の政治家の中にも、メディアの中にもいるかもしれない。そう思いました。』と述べている

（毎日新聞2019年6月20日これが本当なら「現代の特高」…前川元次官が語る告発ノベル「官邸ポリス」のリアル）。まさに、当時の安倍・菅官邸が、公安警察が集めた個人情報によって、政治家や官僚の弱みを握って黙らせるという、独裁的な政治を進めていることが、元事務次官から告発されたといえる。

5 警察組織の政治的中立性が破壊されている

2019年7月15日、札幌で参院選の演説をしていた安倍首相にヤジを飛ばした市民が強制排除されるという事件が発生した。総理に不快な思いをさせないために、総理の演説に対するヤジは取り締まるように、全国の警察組織に対する指令が出ていたとすれば、このような警察権の行使は明らかに警察法2条違反である。

総理の目となり、耳となって官邸を支える内閣情報調査室は、実質的には警察機構のトップに君臨しながら、警察組織ではないという理由で、警察法の軛を免れ、官邸の私兵と化している。そして、安倍政権で長く内閣情報官を務めてきた北村滋氏が、国家安全保障局の局長に就任した。官房副長官の杉田氏が内政を、国家安全保障局長の北村氏が外政を担当することで、菅政権の下で両名とも留任している。官邸は、警察出身者に完全にコントロールされている。

6 日本の監視の歯止めとなる法整備は立ち遅れている

日本政府は、どのような監視技術を持ち、それをどのような要件で使用しているのか、明らかにしていない。アメリカの監視システムの端末は、日本の情報機関も保有しているようである。しかし、それがどのように使われているのか、政府は説明しない。日本企業の多くは、EU の GDPR に準拠しようとしている。

日本にも、個人情報保護委員会がある。しかし、この委員会は企業情報とマイナンバーだけを管轄してきた。今回のデジタル庁法案によって、地方自治体を含む公的機関の全体が、この委員会の管轄の下に置かれることとなった。

2019 年 8 月、この委員会は、めざましい活動を見せた。就職情報サイト「リクナビ」を運営するリクルートキャリア（東京・千代田）が就活生の同意を得ずに「内定辞退率」の予測を顧客企業に販売していた事実を指摘し、8 月 26 日リクルートキャリアに是正を求める勧告を発出したのである。初の勧告だ。リクナビのような大企業で、個人情報の管理がずさんで、プライバシー侵害が起きていたことを明らかにしたのである。

しかし、日本には、公的な個人情報の全体が適切に管理されているかどうかを第三者的な立場で監督できる仕組みが欠けていた。

まず、日本でも、日本版 GDPR を立法化し、すべての公的な情報を含めて管轄する権限を保障された個人情報保護委員会を作らなければならない。日弁連は、ずいぶん以前からそのようなシステムの必要性を訴えてきた。

2015 年 8 月 19 日付の会長声明では、日弁連は「かねてから、専門性が高く、かつ、独立性の強い第三者機関によって、官民を問わず、プライバシーの侵害に対して強い指導監督権限を有する日本版プライバシー・コミッショナーの設立を強く求めてきた。そして、そのような制度がEU等の諸外国においてスタンダードとなっていることを指摘してきた（2014年2月21日付け「日本版プライバシー・コミッショナーの早期創設を求める意見書」等）。」「したがって、行政機関・独立行政法人等について総務大臣が監督する方向で検討することを直ちに改め、法改正後の個人情報保護委員会が官民を一元的に監督する権限を有する制度の創設を行うべきである。」としていた。

第４　個人情報保護確立のための今後の課題

１　個人情報保護委員会の権限と組織の強化が不可欠である

この法改正によって、個人情報保護委員会は、民間だけではなく、行政機関や地方自治体も一元的に管理することとなった。個人情報保護委員会の組織を、少なくとも公正取引委員会並みに、常時800名程度の職員と各地方事務所を有する組織に拡大強化することが必要である。

その権限についても抜本的に強化されなければならない。まずは犯罪捜査と外交防衛分野について、どのような個人情報ファイルが作られているか、個人情報保護委員会に事前に通知する必要がないとする規定を改めることが必要である。

附帯決議によれば、相当の理由や特別の理由による個人データ共同利用ついては、個人情報保護委員会が行政機関を監督するとされている。個人情報保護委員会に行政機関に対する立入調査と命令の権限が認めるべきである。また、個人情報保護委員会の国会に対する年次報告も、従来のものでは全く不十分であり、すべての警察を含む行政機関、地方自治体を対象に厳格な調査を行い、その報告がなされる必要がある。

２　情報機関の監督強化のため、新たな機関の設立が必要である

アメリカには、特定秘密の指定を是正する複数のシステムが機能しており、いったん特定秘密に指定された情報の多くが、一般に公開されている。また、ドイツやオランダには、情報機関の集めた情報を見て、不適切な情報が秘密指定されていればこれを公開させ、あるいは、誤った個人情報が収集されていればこれを訂正させる権限を持ったさまざまな国家機関が活動している。

わが国においては、特定秘密保護法に関連して設立された政府の独立公文書監

理監・国会の情報監視審査会などの機関は十分機能しているとはいえない。公安委員会は公安警察活動に対しては監督できていない。内閣情報調査室、公安調査庁や自衛隊情報保全隊の活動についての監視システムは存在しない。これらの情報機関の活動については、個人情報保護委員会とは別個に、独立した専門の第三者機関が、職権で、特定秘密や情報機関の集めた情報、デジタル庁が共通仕様化した情報等の中身までをチェックし、これに対して是正の勧告・命令ができる制度が必要である。

3　市民による国に対する監視を続けよう

　今回成立してしまったデジタル監視法は、日本の民主主義と人権保障の未来を大きく左右する法律だ。市民と法律家による監視を強め、必要な法改正を要求し、必要な改正がなされないときは、法律の廃止までを求めていく粘り強い運動を続けることを強く呼びかけたい。