JCLU 70周年記念シンポジウム

デジタル時代の監視とプライバシー

― 市民によるコントロールのために ―

2017 年 10 月 1 日（日）一橋講堂

公益社団法人 自由人権協会

JCLU
公益社団法人 自由人権協会
Since1947

シンポジウムの趣旨

2017 年 4 月、クローズアップ現代＋（NHK）で、衝撃のスクープが放映されました。日本政府が、アメリカ政府の監視ツール、XKEYSCORE の貸出しを受けていた可能性を報じるものでした。
同年 2 月には、日本の捜査機関が、10 年近くにわたり捜査活動に GPS 装置を利用しながら、徹底的に秘匿していたことも明らかになりました。

テクノロジーの進化に伴い、政府の監視能力は格段に進歩しています。膨大な情報を集め、管理し、自在に結び合せることが可能となりつつあります。
他方で、政府によるテクノロジーの利用を市民的にコントロールする制度はほとんど変化していません。捜査や防衛の機密を理由として、情報公開もほとんど認められません。旧来のシステムのまま、時代の変化に取り残されています。

JCLU は今年創立 70 周年を迎えました。この間テクノロジーは進化しましたが、私たちの理念は変わりません。市民がそれぞれの人生を生き生きと営むことを可能にするため、自由と人権を守ること。そのために時代にふさわしい制度や理念を提唱すること。

ナショナルセキュリティを理由とする監視は、安全と自由という2つの大切な価値がせめぎ合う最前線です。「国難」が叫ばれる今だからこそ、市民が政府を適切にコントロールすることが必要です。

デジタル時代にふさわしい市民的コントロールの方法を模索するため、このシンポジウムを企画しました。今回の企画を通じて、ご参加いただいた皆様とともにこの問題に対する考えを深め、これからの具体的な取組みにつなげていくことができれば、大変嬉しく思います。

2017 年 10 月 1 日

自由人権協会（JCLU）70周年記念シンポジウム
プロジェクトチーム　一同

プログラム

14:00　**開会挨拶**

14:05　**ライブインタビュー**
米国国家安全保障局による大量監視の実態と日本
エドワード・スノーデン氏
インタビュアー: 国谷裕子氏

15:05　休憩

15:15　**「9.11 以降の監視強化の動きと ACLU の闘い」**
スティーブン・シャピロ氏

15:40　**「日本の監視の現状」**
出口かおり (JCLU 会員・弁護士)

15:55　**「大量監視とプライバシー保護のための仕組み」**
ジョセフ・ケナタッチ氏

16:20　休憩

16:30　**ディスカッション**
コーディネーター: 井桁大介（JCLU 理事・弁護士）

17:25　**閉会挨拶**

※ プログラムの時刻及び内容は都合により変更となる場合があります。

プロフィール

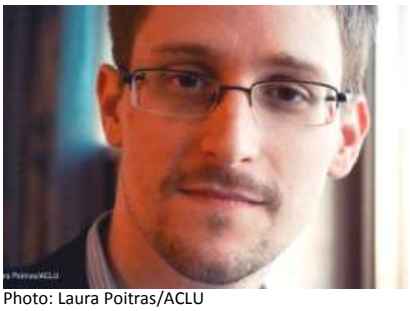
Photo: Laura Poitras/ACLU

エドワード・スノーデン　Edward Snowden

CIA、NSA 及び DIA の元情報局員。テクノロジーとサイバーセキュリティの専門家。2013 年、NSA がテロと無関係な数十億の個人情報を収集していたことを暴露。米国政府が監視政策を修正する大きな転換点となった。

国谷裕子　Hiroko Kuniya

1979 年、米国ブラウン大学卒業、1981 年、NHK 総合〈7 時のニュース〉英語放送の翻訳・アナウンスを担当。1987 年からキャスターとして NHK・BS〈ワールドニュース〉、〈世界を読む〉などの番組を担当。1993 年から 2016 年まで NHK 総合〈クローズアップ現代〉のキャスターを務める。

スティーブン・シャピロ　Steven Shapiro

弁護士。1993 年から 2016 年までアメリカ自由人権協会リーガル・ディレクターを務める。約 90 名の常勤弁護士を指揮し、表現の自由、プライバシーその他多彩な訴訟を取り扱ってきた。コロンビア・ロースクール非常勤教授。

出口かおり　Kaori Deguchi

弁護士。JCLU 会員。日弁連情報問題対策委員会委員。東京弁護士会人権擁護委員会委員。違法な職務質問に対する国家賠償請求訴訟などを手がける。

ジョセフ・ケナタッチ　Joseph Cannataci

2015 年 7 月よりプライバシー権に関する国連特別報告者。IT 法及びプライバシー法の専門家。マルタ大学・フローニンゲン大学教授。2017 年 5 月、共謀罪法案に対する懸念を表明する書簡を安倍首相に送付した。

井桁大介　Daisuke Igeta

弁護士。JCLU 理事。ニューヨーク大学でナショナルセキュリティ法について研究。ムスリム違法捜査弁護団メンバー。

用語集

メタデータ

通信内容以外の情報。電話で言えば、いつ、誰が、誰に対して、どれくらいの時間、通話したかに関する情報。位置情報が含まれる場合もある。

電話のメタデータ収集プログラム

アメリカ政府がアメリカ中の全ての電話のメタデータを毎日収集していた監視プログラム。ターゲットを絞らず無限定に個人情報を収集する典型的なマスサーベイランス（大量監視）の手法のひとつ。

第三者法理（Third Party Doctrine）

第三者に開示された情報は、プライバシーの期待が及ばないとするアメリカの判例法理。電話のメタデータを収集する際の正当化根拠とされた（電話のメタデータは通信のシステム上当然に電話会社に開示されるため）。

PRISM（プリズム）

9 つの大手コンピュータ・IT 会社（Microsoft、Yahoo、Google、Facebook、Paltalk、YouTube、AOL、Skype、Apple）に対し、保有する顧客データの提出を命じるプログラム。対象データの種類は多岐にわたり、メール、チャット、音声通話、ビデオ通話、ストレージに保存されたデータ、送受信されたファイル、ログイン情報、SNS の詳細情報など、あらゆる情報が含まれる（通信内容も含む）。

Upstream（アップストリーム）

光ファイバーケーブルなどインターネット通信が送受信される装置・施設に、政府職員が直接アクセスし、ターゲットとする情報を収集する監視プログラム。対象とする情報は PRISM と類似。

大統領令 12333 号

アメリカ政府における情報機関の活動ガイドライン。アメリカ人や国内を対象とする捜査に対してはプライバシー等に配慮する規定がある一方、国外の外国人の情報を取得する捜査に対しては手続、方法、対象等に関する制約がなく、無限定な捜査を許容する構造となっている。

XKEYSCORE（エックスキースコア 又は 単にエックス）

アメリカ政府の監視ツール。監視プログラムにより収集された情報のデータベースであり、検索エンジンであり、使い勝手のよいユーザーインターフェイスを誇るソフトウェア。スパイの Google と称される。2017 年 4 月に NHK と The Intercept の共同スクープにより、「第三者版」が日本政府に貸し出されていた可能性が報じられた。

合衆国憲法修正4条

「不合理な捜索及び逮捕・押収から、その身体・家屋・書類及び所有物の安全を保障される人民の権利は、これを侵してはならない。宣誓または確約によって証拠づけられた相当の理由に基づくものであって、捜索すべき場所及び逮捕すべき人または押収すべき物件を特定して記載するものでなければ、いかなる令状も発してはならない。」

アメリカにおけるプライバシー法理の根拠法。

欧州人権条約8条

「プライバシー、家庭生活、住居、通信に関して尊重される権利を有する」

欧州におけるプライバシーの根拠法。

FISA（The Foreign Intelligence Surveillance Act of 1978 / フィサ 又は ファイザ）

外国諜報活動監視法。外国を対象とする諜報活動に関する手続について定めたもの。

FISC（Foreign Intelligence Surveillance Court / フィスク 又は ファイザ・コート）

FISAにより設立された特別裁判所。11人の連邦裁判官から構成される。FISAに基づく諜報活動について令状審査などの監督を行う。

愛国者法（Patriot Act / パトリオットアクト）

9．11の直後にテロ対策権限を強化するために制定された。アメリカ中の電話のメタデータを収集するNSAのプログラムは、同法215条が法的根拠とされた。

FAA（FISA Amendment Act）

2008年FISA改正法。PRISMやUpstreamは同法の702条が根拠とされている。

PCLOB（Privacy and Civil Liberties Oversight Board）

行政内部の独立機関。スノーデンリーク後、電話のメタデータの収集プログラム、PRISM 及びUpstream について、機密情報にアクセスした上で、適法性と政策の妥当性に関する詳細な監督レポートを公表した。

Jones事件（2012年）

本人に無断でGPSを利用して位置情報を取得する捜査活動の違憲性について論じた判決。少数意見により第三者法理の見直しが提案された。

Riley事件（2014年）

通常の携行品であれば逮捕に伴い差し押さえることが許されるが、携帯電話の中身を見るには令状を必要とするとした判決。携帯電話がプライバシー情報の塊であることを重視したもの。

講演アウトライン　スティーブン・シャピロ

（和訳）

「9.11 以降の監視強化の動きと ACLU の闘い」

アメリカ自由人権協会　全米リーガル・ディレクター(1993-2016)
スティーブン R.シャピロ

1. イントロダクション

- 「プライバシー」の言葉は、米国合衆国憲法の条文には出てこない。歴史的には、プライバシーの概念は財産権及び不法侵入の法理と結びついていた。
- 連邦最高裁は、カッツ対合衆国事件（1967 年)において、憲法が保護しているのは場所ではなく人々であって、それゆえ政府は個人の「プライバシーに対する合理的な期待」を侵害する前に、原則として令状を得なければならないという理論に基づき、不合理な捜索差押に対する憲法上の保護は、公衆電話を用いた会話の盗聴に適用されると判示した。
- カッツ判決がちょうど 50 年前に出てから、技術発展により、政府（及び産業界）は、我々の私的生活の詳細について監視、収集、保存及び分析することができる、事実上無限の能力を有するに至っている。
- 米国法は未だこの技術革新に追いつくことができていない。私たちはデジタル世界に生きているが、ほぼアナログ世界に発展してきた憲法理論に未だに依拠し続けている。
- 9.11（2001 年米国同時多発テロ）後、政府はその監視の能力とプログラムを拡充していることから、これらの問題を解決する緊急性は極めて高まっている。

2. 解決されていない問題

- どの時点でプライバシーは侵害されるか――政府があなたに関する情報を収集したときか、政府がそれを検討対象にしたときか、又は政府がその情報を使ってあなたに不利な行動をとったときか。
- あなたがインターネットプロバイダーなどの第三者とあなたの情報を共有したという事実は、もはやそれが私的なものではなく、それゆえ政府がアクセスできる情報になることを意味するか。
- ナショナルセキュリティのための監視と、犯罪捜査のための監視とでは、異なるルールが適用されるべきか。
- 「プライバシーに対する合理的な期待」という枠組みは、新しいデジタル時代でも採用できるか、あるいは私たちは新しい憲法上の枠組みを必要としているか。

3. ACLU の目指すもの

- 透明性、説明責任及び司法審査
- 透明性：アメリカ国民は、政府が自分達を密かに監視する場合これを知る権利がある。
- 　特定の個人は、ナショナルセキュリティ絡み又は犯罪の捜査の対象になっている場合、少なくとも初期の段階においてはそのことを知る権利はないかもしれない。しかし、政府が何百万人もの人のメールや電話のメタデータを集めているのであれば、異なった利益衡量が適用される。人々が知らなければ、確かな情報に基づく公共の政策論争は存在しえない。
- 司法審査：憲法規範を確立するために不可欠である。
- 説明責任：憲法規範を実行するために不可欠である。

4. ACLU の 9.11 後の活動

- 前提は、監視用ツールは引き出しの中にしまわれたままではないということだ。利用可能なツールは使われる。法の支配が及んでいなければ、監視ツールはほぼ間違いなく濫用される。
- 9.11 後の監視活動についての私たちの知識は主に2つの情報源による。内部告発と情報公開法に基づく請求である。
- ACLU の依頼者であるエドワード・スノーデンは、政府による監視についての適切な制約に関する公的議論を引き起こし、内部告発の重要性を示した。これは他の方法では実現しえなかったことで、すでに重要な政策変更をもたらしている。
- ACLU の情報公開活動は、ACLU のスパイ・ファイル・キャンペーンとして広く集約され、平和的な政治的抗議者及びイスラム教のコミュニティその他を対象にした監視活動を明らかにするのに役立った。

5. 主な ACLU 関与事件

- ACLU 対クラッパー事件（2015 年） －愛国者法 215 条に基づく電話のメタデータ大量収集の違法性を争い成功。米国自由法の制定を導く。
- アムネスティ・インターナショナル USA 対クラッパー事件（2012 年）－原告の通信が、問題のプログラムの下で監視対象になることが確実であることを立証できていないとして、2008 年 FISA 改正法 702 条について争う当事者適格（standing）を否定された。
- ウィキメディア対国家安全保障局事件（2017）－連邦控訴裁判所は、2008 年 FISA 改正法 702 条に基づく「アップストリーム」による監視の違憲性を争うことを許容した。
- カーペンター対合衆国事件（今秋に弁論予定）－147 日間にわたって被疑者の携帯位置情報を入手するために、合理的な根拠に基づく令状が必要か否か。

6. 結論

- 訴訟の結果は様々である。しかし、たとえ裁判所でうまくいかなくても、訴訟は問題にスポットライトを当て、公の議論を生み、政治的変化の触媒となる可能性がある。
- 私たちは既に、10 年前には想像もつかなかった監視国家に生きている。私たちはプライバシーの喪失について諦めることなく、プライバシーを失わないようにする努力を精力的にたゆむことなく続けていかなければならない。

講演アウトライン　スティーブン・シャピロ

“THE ACLU’S FIGHT AGAINST ENHANCED SURVEILLANCE AFTER 9/11”
Steven R. Shapiro
National Legal Director, ACLU (1993-2016)

1. Introduction

- The word “privacy” does not appear in the US Constitution. Historically, the concept of privacy was tied to property rights and the law of trespass.
- In *Katz v. United States* (1967), the US Supreme Court held that the constitutional protection against unreasonable searches and seizures applies to a wiretapped conversation in a public pay phone on the theory that the Constitution protects people, not places, and therefore the government must generally obtain a warrant before violating an individual’s “reasonable expectation of privacy.”
- Since *Katz* was decided exactly 50 years ago, technological developments have provided government (and industry) with a virtually limitless capacity to monitor, collect, store, and analyze the details of our private lives.
- US law is still struggling to catch up with this technological revolution. We live in a digital world but continue to rely on a constitutional jurisprudence that was largely developed in an analog world.
- The urgency of resolving these questions has increased significantly since 9/11 as the government has expanded its surveillance capacities and programs.

2. Unanswered questions

- At what point is your privacy invaded: When the government collects information about you, when it reviews that information, or when it uses that information to take some action against you?
- Does the fact that you have shared your information with a third party, including your Internet service provider, mean that it is no longer private and thus accessible to the government?
- Should a different set of rules govern national security surveillance and criminal surveillance?
- Can the “reasonable-expectation-of-privacy” framework be adapted to the new digital age or do we need a new constitutional standard?

3. ACLU goals

- Transparency, Accountability, and Judicial Review.
- Transparency because the American people have a right to know when the government is spying on them. Specific individuals may not have a right to know if they have become targets of a national security or criminal investigation, at least at the early stages. But a different balance applies when the government is collecting emails and telephone metadata for millions and millions of people. There cannot be an informed public policy debate if people are not informed.
- Judicial review because it is essential to establish constitutional norms.
- Accountability because it is essential to enforce those norms.

4. ACLU Activities Post-9/ll

- Operating premise: Surveillance tools never sit in a drawer. If they are available, they will be used. And, unless subject to the rule of law, they are almost certain to be abused.
- Our knowledge of surveillance efforts post-9/ll primarily comes from two sources: leaks and Freedom of Information Act requests.
- Ed Snowden, who is an ACLU client, has demonstrated the importance of leaks in provoking a public discussion about the appropriate limits on government surveillance that would not otherwise have occurred and that has already led to important policy changes.
- The ACLU's FOIA efforts, broadly consolidated under what we have described as the Spy Files Campaign, have helped to reveal surveillance activity targeted at peaceful political protestors and the Muslim community, among others.

5. Selected ACLU cases

- *ACLU v. Clapper* (2015) – successful statutory challenge to mass collection of telephone metadata under Section 215 of the Patriot Act, leading to passage of USA Freedom Act.
- *Amnesty International, USA v. Clapper* (2012) – no standing to challenge Section 702 of the FISA Amendments Act of 2008 because plaintiffs could not establish that their communications were certain to be subject to surveillance under the challenged program.
- *Wikimedia v. NSA* (2017) – federal appeals court allows challenge to Upstream surveillance under Section 702 to proceed.
- *Carpenter v. US* (to be argued this fall) – whether a probable cause warrant is needed to obtain a criminal suspect's cell site location information (CSLI) for 147 days.

6. Conclusion

- The litigation record has been mixed. But even when we do not succeed in court, litigation can shine a spotlight on a problem, generate public discussion, and be a catalyst for political change.
- We already live in a surveillance state that would have been unimaginable a decade ago. We must not become resigned to the loss of personal privacy, but we must be tireless and vigilant in our efforts to preserve it.

報告　日本の監視の現状

日本の実態は・・・？

出口かおり

1．日本の「情報機関」

○ 独立したインテリジェンス機関はなく、監督する仕組みもない
○ 犯罪の嫌疑を前提としない情報収集活動を行う国家行政機関が複数あり、それぞれが独自の目的で活動している：内閣情報調査室、防衛省情報本部、公安調査庁
○ 警察制度は、法律上は自治体警察だが、各自治体警察の幹部は、国家行政機関たる警察庁から派遣されていることが多く、かつ、階級制をとった上意下達の組織形態であることから、事実上、各自治体警察の独立性は乏しく、国家警察に近い状態
→ 警察が、犯罪の嫌疑を前提とした捜査活動のみならず、これを前提としない警備公安活動も担当している
→ 警備公安を担当した警察官僚が、内閣情報調査室や防衛省情報本部に出向している
○ 犯罪の嫌疑を前提としない国家行政機関や警察の情報収集活動を行う権限を付与した明示的な法律上の規定はなく、警察は警察法2条[1]といったきわめて抽象的な規定を根拠にしている

2．拡大する警察による情報収集

（1）公権力による情報収集活動に関する法律の規定は多くない

○ 通信傍受法
一定の犯罪の捜査に必要な場合にのみ、裁判所の令状に基づき認められる。
傍受した通信の全てと傍受の経過が自動的に記録されるから、捜査機関が濫用しても事後的に検証可能というが、果たして実効性があるか？
○ 特定の嫌疑を前提としながら、「強制捜査」ばかりでなく「任意捜査」での情報収集が多い
・ 法律ではなく規則に基づいて「任意に」収集される指紋・顔写真・DNA 型情報
→ 収集できる犯罪に限定はなく、軽微な犯罪でも、被疑者とされた者は、多くの事案で「任意に」指紋・顔写真・DNA の採取に応じるよう「説得」される。
・ 民間企業や行政機関は、警察の依頼があれば、令状がなくとも、任意に個人情報を提供するところも多い
→ 警察の内部決裁だけで発出できる捜査事項照会書を示せば、民間企業及び行政機関のほとんどが対象者の個人情報を提供しており、必要性等が認められない等を理由に拒否する事例は少ないと思われる。
・ 民間企業や行政機関で、LINE のように、捜査事項照会の件数など、捜査機関への情報提供の実態を公表している企業はほとんどない。
・ 監視カメラについても法的規制がない。民間が設置したもののほか、警察が設置したものもあるが、いずれも、入手した映像をどのように利用・保存しているか、あるいは必要のない情報を消去しているかは明らかにされていない。

---

1 警察法2条（警察の責務）
警察は、個人の生命、身体及び財産の保護に任じ、犯罪の予防、鎮圧及び捜査、被疑者の逮捕、交通の取締その他公共の安全と秩序の維持に当ることをもつてその責務とする。
2 警察の活動は、厳格に前項の責務の範囲に限られるべきものであつて、その責務の遂行に当つては、不偏不党且つ公平中正を旨とし、いやしくも日本国憲法 の保障する個人の権利及び自由の干渉にわたる等その権限を濫用することがあつてはならない。

報道によれば、2014 年から、警視庁等の全国5都県に顔認証装置も導入された。

→ 警察が、入手した画像をすでに顔認証解析している可能性もある。

○ GPS捜査も法律の根拠なく、かつ、秘密裡に行われていた。

→ 2017 年 3 月 15 日最高裁判決は、対象者の承諾なく密かに GPS 端末を取り付けて位置情報を検索し把握する GPS 捜査は、「個人の行動を継続的、網羅的に把握することを必然的に伴うから、個人のプライバシーを侵害し得るものであり」「公権力による私的領域への侵入を伴うもの」であるから、任意捜査ではなく、強制処分に当たるとした。

個人のプライバシーを侵害する捜査手法は、法律の根拠がなければ許されない、と裁判所が述べた意義は大きい。「私的領域」に侵入するITを使った様々な捜査手法にも当てはまる考え方である。

なお、警察庁は 2006 年に GPS 捜査に関する「保秘の徹底」を指示し、10 年以上にわたり秘密裡に違法な捜査が行われていた。

○ 捜索差押時の広汎なデジタル情報の収集

デジタルデータは、媒体の外見からだけでは犯罪に関係があるかどうかがわからないという理由で、携帯電話の情報、捜索差押えで押収したパソコンやハードディスク内のデータを、捜査機関が可能な限り全てコピーし、保存している可能性が高い。

(2) 捜査機関における個人情報の取扱いについての法的規制が有効でない

捜査機関が入手した個人情報をどのように管理・利用・保存しているかは明らかにされず、個人情報の保存・利用・管理が事実上自由になされている

→ 指紋・顔写真・DNA 型情報はそれぞれデータベース化され、一度登録されると、「必要が無くなった」と捜査機関が判断するまで登録され続け、登録された者が抹消請求する手続や、登録されているかどうかを確認する手続はない。

→ 暴力団員・暴力団関係者のデータベース(いわゆるB登録)もあり、一度登録されると抹消困難。B登録されたと思われる人物が、銀行で口座開設を理由も明らかにされずに拒否されたり、職務質問で執拗に調べられたりする事例がある。

※ XKEYSCORE などのプログラムが防衛省に提供か

スノーデン氏が公開した文書に、国家安全保障局が日本の諜報活動支援に XKEYSCORE などの諜報プログラムを防衛省情報本部電波部に提供したとの記載があった。これについて、防衛省は回答していない。

(3) 今後、捜査活動名目での情報収集活動が増えるおそれがある

○ 共謀罪の成立

準備行為等の共謀罪の成立要件が曖昧なため、犯罪とは無関係な日常の行為を「犯罪の準備行為」と見ることができるとの懸念がある。加えて、共謀の有無を捜査するとの口実で、民間人の通信内容等の提供を警察が求めたり、捜査対象者が外で会う人物を確認するとの名目で民間が設置した監視カメラの画像の提供を警察が求めることができるようになる。

→ 特定の犯罪の証拠を確認した上で捜査を行う従前の手法ではなく、「怪しい」人物の行動をマークして、犯罪がないかを探す捜査手法が増えてゆくおそれがある。

犯罪予防を目的とする行政警察活動と司法警察活動の伝統的区分が曖昧になり、刑事事件の捜査活動と公安活動の区分も曖昧になってゆく。

3. デジタル時代の監視

以上の状況から、現在、警察がターゲットにすると決めた市民の様々な個人情報を、本人が知らないうちに集めることができる状況にある。

犯罪と関係ないとわかっても、集めた情報を削除していない。

テロ対策を理由に収集した個人情報が、具体的にテロ対策にどのように有効であったかの検証もない。入手した情報をどのように利用・保存しているかもわからない。

科学技術の進化により、個人の生活に伴い様々なデータが生み出されるようになった一方、これらのデータを警察が収集・保存・利用する法的根拠や必要性・有効性について、日本ではほとんど議論されていない。

スノーデンリークは、国家が行う情報収集活動について、市民が関心を持ち、議論することの重要性を教えてくれた。

日本は、捜査と諜報活動はいずれも警察が行い、「任意捜査」を理由に、警察が様々な個人情報を集めているが、市民が気付かないところで行われているために実態がわからず、国家も説明しようとしない。濫用を防ぐためにも、まずは情報収集の法的根拠を明確にし、収集した情報の管理・保存ルールを作ることが必要である。

さらに、濫用の疑われる情報収集活動について、国家が運用状況を毎年説明したり、第三者機関が活動を検証して市民に報告するなど、市民がその活動実態を知り、議論することができる体制づくりも求められる。

＝＝

〈 参考情報 〉

日本の情報公開法

日本の情報公開法は 2000 年から施行された。特徴的な問題点として、

①訴訟でインカメラ審理が認められていない

②不開示要件が曖昧で広範

③原告が勝訴しても弁護士費用は補償されない

ことなどをあげることができる。

②について、特に外交上の機密情報や公共の安全に関する情報の不開示事由は、

「公にすることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあると行政機関の長が認めることにつき相当の理由がある情報」、

「公にすることにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがあると行政機関の長が認めることにつき相当の理由がある情報」

という条文であり、行政機関の長の裁量を広く認めるかのような書き方になっている。

日本で集められている主な個人情報

（1） 警察以外の行政機関が保有する個人情報

・戸籍：出生から死亡までの家族関係がわかる。戸籍を集めることで家系図を作ることができる。

出自や、結婚した両親のもとに生まれたか、結婚していない女性の子として生まれたか、兄弟姉妹は何人いるか、養子か実の子かなど、他人に知られたくないこともわかってしまう。

原則として、本人と同じ戸籍に入っている親族しか開示請求できないが、警察は「捜査の必要」があれば入手できる。過去には、特定の犯罪と関係なく、市役所にある住民基本台帳の情報を警察官が日常的に自由に閲覧していたことが発覚した事例もある。

・住民票：現在の住所地がわかるもの。

・収入額：自治体が住民に税金を課すための基礎情報として、勤務先等から年収額の提供を受ける。

・その他、ある人が生活保護や介護、障害者認定を受けているか等も、行政機関に情報がある。

（2） 検察庁や警察署が保有する個人情報

・前科前歴情報

・「強制」或いは「任意」に収集された被疑者指紋や顔写真、DNA 型情報

・Nシステム（自動車ナンバー自動読取装置）～法的規制はない

全国の所定の地点を通過する車両全てについて、運転者や同乗者も含めてカメラ撮影して保存する警察庁管理のシステム

・運転免許証の顔写真画像、本籍地情報

（3） 民間企業等が保有する個人情報

・電話番号や通話履歴

・銀行口座の取引履歴

・金融機関からの借入・返済履歴

・クレジットカード利用情報

・監視カメラ映像（店舗、ATM、タクシー、駅、路上、個人宅等）

・病院のカルテ記録

・ネットショッピングの利用履歴

・メールの通信記録

・携帯電話の位置情報　など