論　説

言論規制―従来型と最新型(2・完)

Jack M. BALKIN
石新　智規・樫尾　　洵(訳)

B．デジタル事前抑制

1．従来型：伝統的な事前抑制及びその効果―出版初期の時代に遡る、最も古い形の言論規制の1つが事前抑制である[73]。今日、事前抑制は一般的に司法による差止め（*Pentagon Papers* 事件における論点）に伴うものであるが、そのルーツは、印刷機を稼働させるために国家が許可の取得を要求し、出版前にコンテンツの事前検査を要求する、より古い許可制及び官僚機構にある[74]。

Pentagon Papers 事件における政府の差止請求は世の中とコミュニケーション技術に関する一定の事実を前提としており、その前提事実によって差止めは取得する価値のあるものとなっていた。すなわち、差止めの請求は、例えば、Pentagon Papers 社が新聞の印刷及び印字を行う時間がある場合のみ、出版を行うことができることを前提とした。それは、原本の複製を作ることにはかなりの時間と労力を要すること、そして、Daniel Ellsberg が複数の新聞の電子コピーを作成し、アメリカの裁判所の管轄を越えて世界中に瞬く間にそれを広めるという、当時では魔法の能力を持たないことを前提としていた。

---

[73] *See* FREDRICK SEATON SIEBERT, FREEDOM OF THE PRESS IN ENGLAND, 1476-1776, at 21-30 (1952).

[74] *See* Philip Hamburger, *The Development of the Law of Seditions Libel and the Control of the Press*, 37 STAN. L. REV. 661, 673 (1985)（「許可は多くの利点をもたらした。特に、出版物のコントロールのために用いられる場合、許可制は国王が出版前の検閲をすること及び侵害者を簡単に処罰することを可能にした。」）.

政府が*Pentagon Papers*事件のように司法的差止めを通して機密情報を抑制し得るという考え方は、今日ではほとんど古風で変わったものに見える。現代のDaniel Ellsbergは海外の多くの異なる場所に安全なサーバーを持つWikiLeaksのような組織と協力するであろう[75]。逆にWikiLeaksは、公開によるリークを実行するために世界中の異なる国の格式のあるニュース組織と協力するであろう（また実際に協力してきた）。WikiLeaksの電信が公表を始めたとき、オバマ政権はニクソン政権のように差止めを求めようとはしなかった。代わりに、オバマ政権はWikiLeaksをコントロールするための異なる方法に頼った[76]。

それにもかかわらず、デジタル世界においても、事前抑制（一方当事者のみからの聴聞による差止めを含む）は、正しく使われれば言論規制の重要な道具になり得る。また、新たな言論規制の最も重要な機能のうちのいくつかは、許可制や司法的差止めを用いない場合でも、伝統的な事前抑制に類似する効果を得るためにデジタル技術を取り入れている。それゆえ、これらの最新型の手法を論じる前に、事前抑制がどのように作用し、なぜ事後の刑事訴追よりも出版の自由を制限するのかについて理解することが重要である[77]。

事前抑制（許可制を含む）は、裁判のコスト、証明責任及び不作為の結果を国家から表現者に移転させるため、特に問題である。事前抑制は有害なコンテンツを容易に発見、ブロック及びコントロールできるようにしようとし、また侵害を行う表現者を容易に起訴、処罰及び抑止可能とする。これらの効果は6つのカテゴリーに分けられる。

---

[75] MICAH L. SIFRY, WIKILEAKS AND THE AGE OF TRANSPARENCY 27-28, 37 (2011); Noam Cohen, *What Would Daniel Ellsberg Do with the Pentagon Papers Today?*, N.Y. TIMES, Apr. 19, 2010, at B3.

[76] *See infra* section II.C.2.c, pp. 2327-29.

[77] 修正第1条から見た事前抑制の問題点に関する標準的な議論については、see Thomas I. Emerson, *The Doctrine of Prior Restraint*, 20 LAW & CONTEMP. PROBS. 648, 656-60 (1955), *see also* Stephen R. Barnett, *The Puzzle of Prior Restraint*, 29 STAN. L. REV. 539 (1977); Vincent Blasi, *Toward a Theory of Prior Restraint: The Central Linkage*, 66 MINN. L. REV. 11 (1981); John Calvin Jeffries, Jr., *Rethinking Prior Restraint*, 92 YALE L.J. 409 (1983).

(a) 意図的に広げられる適用範囲―まず、事前抑制は事後の起訴及び罰則のシステムよりもずっと広くかつ多様なコンテンツを政府規制及び監視の対象とする。検察官や民事の原告は、その注意を引いた行為のみを検討し、提起するかどうかを決める必要がある。事前抑制のシステムでは、どれだけ問題がないものであったとしても、全てが政府の前に晒され、出版される前に政府の許可を必要とする。事前抑制の長所であり、同時に短所となるのは、保護されるコンテンツも保護されないコンテンツも一緒にまとめられることである。

(b) 活動しないこと及び不作為の負担の移転―第二に、事前抑制のシステムでは、コミュニケーション（修正第１条の下で完全に保護されるコンテンツのコミュニケーションを含む）は許可が得られるまで起こり得ず、このことはメッセージが伝達されることによる効力や価値を損なう可能性がある。国家の許可を得る義務が表現者に課せられている。政府が反応せず、許可も与えなければ、表現者は沈黙させられる。事後処罰のシステムでは、表現の遅延は生じず、規制を行う場合、国家は反応する義務を課せられる。国家が何もしなければ自由表現は継続する。このように、事前抑制を行うことは、かなりの量の保護された素材を、保護されない素材を探すことを促進するために無制限にブロックし続ける可能性があるため、(規制の）範囲が広すぎるという問題を悪化させる。

(c) 限定的な手続保障及び別の司法手続に対する決定の先送り―第三に、事後処罰のシステムは表現者に、陪審員による裁判、言論の自由の憲法的保護を含む、完全な手続保障を可能とする機会を与える。事前抑制のシステムは行政的又は非公式なものとなる可能性があり、問題はコンテンツが修正第１条で保護されているか否かではなく、行政官が関連する制定法のカテゴリーにコンテンツが該当すると考えるかどうかになってしまう。執行官又は行政官が決定を行い、当該決定は行政行為に対する、より限定された司法審査の対象にしかならない可能性がある。更に、デジタル時代においては、決定は人間の関与なしにソフトウェアプログラムによってなされる可能性があり、実効性のある司法審査の方法がないということもあり得るかもしれない。

(d) 公開される訴追から可視性の低いコントロールシステムへの移行―第四に、事前抑制のシステムは公衆による審査の及ばないバックグラウ

ンドで作用し得る。それは事務として習慣化され、組織化され得る。この問題は、デジタルコンテンツのブロッキングやフィルタリングが自動化される場合に大きくなる。事後処罰のシステムは多くの場合、刑事又は民事を問わず、訴追するために個別の決定を要求する。これは、訴追の実行が賢明か否かについて、より多くの審査及び議論の機会を公衆に与える。

（e）誤りのコストの負担の移転―第五に、事前抑制のシステムは行き過ぎた検閲への制度的な動機を作り上げる。Thomas Emerson 教授がかつて説明したように、「検閲の役割は検閲である」。それは抑制するものを探すことに専門的な興味を持っている。それはしばしば抑制を求める利益（それ自身が代表する利益）に敏感に反応し、自由表現を支える、より分散し消極的な力にはそれほど同調しない[78]。これは、停止のための権力が私人の手に担われ、又はフィルタリングプログラムで自動化されている場合、よりよく当てはまる。

（f）自己識別の強制、すなわち所在の特定、逮捕、抑制及び処罰の可能性の増加―第六に、事前抑制は、政府が関心を持つコンテンツがより抑制され、またその出版社が特定され処罰されるように設計されている。事後処罰のシステムでは、政府は有害なコンテンツを見付ける必要があり、また訴追がそれに要する時間と手間に値するかについて決定する必要がある。事前抑制のシステムは費用の負担を政府から表現者に移転し、検閲のコストを下げる。表現者は、なぜそのコンテンツは出版されるべきなのか証明する負担を課される。

もし表現者が事前抑制システムの許可制度を無視し、又はこれに逆らえば、主な問題は、コンテンツが憲法的に保護されているかどうかではなく、表現者が正しい許可を事前に得たかどうかになる。これが、裁判所の差止めを事前抑制のように作用させる中核的な特徴である[79]。付随的審査制の下では、もしある者が裁判所の出版差止命令に違反したら、出版者は通常、法廷侮辱罪に対する防御として裁判所の命令の違憲性を争う権利を失う[80]。

---

[78] Emerson, *supra* note 77, at 659.

[79] Jeffries, *supra* note 77, at 431-32（差止めを事後処罰より問題があるものとする特徴の 1 つは、付随的禁止ルールの継続的な持続であると論ずる）.

[80] Richard E. Labunski, *The "Collateral Bar" Rule and the First Amendment: The Consti-*

更に、誰かが法に違反したと疑う検察官は通常その違反を個人的な侮辱とは捉えない。むしろ、その検察官は訴追を行うことが所与の有限なリソースの下で行われる努力に値するかについて専門的な計算を行う。一方で、もし表現者が事前抑制システムにおいて許可を得なかった場合、許可を与える者（差止めの場合は裁判官）は、その行為を彼らの権威に対する脅威と見て、彼らの権力を確立するために確実かつ厳しい処罰を好むであろう。

２．最新型：デジタルインフラストラクチャーに向けられた事前抑制―デジタル技術は、行政又は官僚機構による審査方法、又は司法による差止めを必ずしも必要としない手法を通じて、国家及びそれに協力的な私人の両方に、事前抑制に関する多くの費用や負担の移転を可能とする。

(a) フィルタリング―フィルタリングシステムはテクノロジーを用いて伝統的な事前抑制と同じ効果を得る。フィルタリングシステムは、特にDNS又はIPレベルで行われる場合、しばしば範囲が広すぎる[81]。しかし、範囲が広すぎることは、特に費用の削減と包括的な効果を得ることが目標である場合においては、特長であり欠陥ではない。

フィルタリング技術は、リバースエンジニアリングを防ぐため、しばしば秘密とされ、営業秘密保護法により保護されることもある。フィルタリング基準は、特に国家が私人により設計されたフィルターを使う場合、修正第１条の分類を尊重していなかったり、内容又は見解を基準とする不適切な規制となっている可能性がある[82]。フィルタリングシステムはフィル

---

tutionality of Enforcing Unconstitutional Orders, 37 AM. U. L. REV. 323, 327 (1988)（付随的な禁止のルールについて説明する）. 裁判所は命令が「明白に無効」である場合はルールが適用されるべきではないと論じて、厳格さを緩和するためにその法理に例外を継ぎ足している。*See* Walker v. City of Birmingham, 388 U.S. 307, 315 (1967)（付随的禁止ルールを適用し、「これは差止めが明白に無効、又は有効であるとほぼ考えられない事案ではない」と論じる）. *In re* Providence Journal Co., 820 F.2d 1342, 1347 (1st Cir. 1986)（「明白に無効な命令が不服従罪の召喚状の根拠となることはない。」）.

[81] Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 397 (2009)（「全てではないとしても、ほとんどのインターネットフィルタリングシステムは過度に広範に規制する（無害なコンテンツをブロックする）か、規制が狭すぎる（禁止されている素材をブロックできない）か、又はその両方かである。」）.

[82] 国家の行為がない所にはコンテンツ及び視点に基づいたフィルタリングを行っ

ターに抗議する機会、表現者への手続保障又はブロックされる言論の個別の憲法的分析なく、言論を自動的にブロックする[83]。誤った判断に伴うコストはフィルタリングシステムではなく表現者に課され、ブロックの結果を変更し又は除去する負担は表現者にある。最後に、フィルタリングシステムはバックグラウンドで静かに働き、それらの効果は一般公衆には気付かれないであろう[84]。

(b) ドメインネームの差押え―国家は、数字のIPアドレスとwww.nytimes.comのようなドメインネームを繋げるドメインネームシステムへのコントロールを主張することで、コンテンツをコントロールすることができる。例えば、2010年11月、国土安全省（Department of Homeland Security）は、知的財産権を侵害したと疑われる人物や事業体のドメインネームを差し押さえるOperation In Our Siteをスタートした[85]。

ドメインネームの差押えは、伝統的事前抑制と少なくとも5つの特徴を共有する。まず、それは設計の段階から規制の範囲が広すぎる。ドメインネームシステムを無力にすることは、あるドメインネームにより辿り着くことができる全てのコンテンツをブロックすることである。第二に、それ

ている私的当事者に対する憲法上の疑義を出す余地はなく、Section 230の規定の中には、コンテンツをブロックすることについてさえ仲介者を免責するものがある。47 U.S.C. § 230 (c)(2) (2006). しかし、コンテンツ又は視点に基づいたフィルタリングが政府による付随的検閲により発生する場合は、国家行為があることになる。*See* Balkin, *supra* note 39, at 2299.

[83] この点は知的財産の文脈において特に重要である。多くの最新の言論規制は著作権の潜在的な侵害に向けられている。「(特定の出版に対する）事前抑制は、明らかに有効な著作権に対する差し迫った侵害についての一般的な司法上の反応である」Dall. Cowboys Cheerleaders, Inc. v. Scoreboard Posters, Inc., 600 F.2d 1184, 1187 (5th Cir. 1979)（裁判例をまとめている）が、それは、(侵害に関する司法上の判断に関わらない）事前抑制の行政上又は技術的枠組みが言論の自由の原則を免れることを意味するものではない。

[84] 政府はフィルタリング技術の回避も違法とすることができる。*Cf.* 17 U.S.C. § 1201 (2012)（アクセスコントロール装置を回避するテクノロジーの配布を違法とする）.

[85] NAT'L INTELLECTUAL PROP, RIGHTS COORDINATION CTR., OPERATION IN OUR SITES, http://www.ice.gov/doclib/newsflibrary/factsheetslpdf/operation-in-our-sites.pdf (last visited May 10, 2014), *archived at* http://perma.cc/6KMD-5BTW.

らは不作為及び活動しないことのコストを転換する。当該ドメインネームを通じたアクセスは、政府がドメインネームを修復するまでブロックされる。第三に、一般的にドメインネームの差押えは、影響を受ける当事者に対する手続保障が限られる一方当事者のみに対する審問により発せられる。第四に、ドメインネームの差押えは目立たない行為である。第五に、政府は、ドメインネームの差押えにおいては、度を越して熱心に訴追することに対してはあまり意欲的でない私人とも協働することができる。

ある不幸な事故において、移民関税捜査局（Immigration and Customs Enforcement (ICE)）は、著作権侵害を助長している疑いで、Dajazıが運営していたヒップホップウェブサイトのドメインネームを差し押さえた。差押えは宣誓書によって正当化されていたが、この宣誓書は不正確な情報に基づいていた。特に、差押命令を正当化した、侵害の疑いがあるとされたリンクは、実際はアーティストら自身によってDajazıに与えられていた[86]。しかし、ICE及び司法省は、全米レコード協会（Recording Industry Association of America (RIAA)）と共に働き、当初の命令を何度も非公開かつ一方当事者のみに対する審問によって延長するなどして、サイトを1年間ダウンさせた[87]。最終的に、政府が訴追に進むための合理的疑いが欠けていたと決定した後、差し押さえられたドメインは修復された[88]。

---

[86] Dara Kerr, *Homeland Security's Domain Seizures Worries Congress*, CNET (Sept. 3, 2012, 8:41 PM), http://news.cnet.com/8301-1023_3-57505318-93/homeland-securities-domain-seizures-worries-congress, *archived at* http://perma.cc/9U3Q-CSBT.

[87] *See In the Matter of the Seizure of the Internet Domain Name "DAJAZI.COM,"* ELEC. FRONTIER FOUND., https://www.eff.org/cases/matter-seizure-internet.domain-name-dajazicom (last visited May 10, 2014), *archived at* http://perma.cc/X42D-5NL2（非公開だったが、2014年5月に公開された訴訟記録）; Kerr, *supra* note 86.

[88] *See* Kerr, *supra* note 86; Timothy B. Lee, *Waiting on the RIAA, Feds Held Seized Dajazı Domain for Months*, ARS TECHNICA (May 4, 2012, 11:41 AM), http://arstechnica.com/tech-policy/2012/05/waiting-on-the-riaa-feds-held-seized-dajazı-domain-for-months, *archived at* http://perma.cc/URT7-V56S; *see also* Bambauer, *supra* note 8, at 865-67（司法省及びHomeland Securityが、児童ポルノを含むと考えられていたドメインネームをコントロールするために一方当事者審問に基づく命令を使用し、いかなる犯罪についても無実であったサイトを一掃したOperation Protect Our Childrenについて述べる）.

このエピソードは最新型の言論規制の3つの特徴的な側面を含んでいる。(1) 政府と私人の協力、(2) インフラストラクチャーへの攻撃による言論のコントロール、及び (3) 伝統的手続保障及び自由の保護を迂回する新しい執行テクニックである。

(c) フィルタリング又は付随的検閲の結果をもたらすように設計された差止め―しばしばコンテンツ業界から突き上げを受ける政府は、差止めを新しい方法で用いる、良くできた新しい枠組みを作り上げた。その革新の中心は、表現者を標的とする制約から私的インフラストラクチャーの保有者を標的とする制約への移行である。目的は、私的インフラストラクチャーの保有者に監視、ブロック及びフィルタリングをさせることである。

非常に良い3つの例は、最近のアメリカ合衆国議会で提案された（そして有り難いことに否決された）法律案、すなわちCombating Online Infringement and Counterfeits Act[89]（COICA）、Stop Online Piracy Act[90]（SOPA）及びPROTECT IP Act of 2011[91]（PIPA）である。これらの議案は、知的財産権に損害を与える素材を供給しているだけの海外のウェブサイトを規制、ブロック、又は処罰するというはっきりとした目的を有していた。一方で、その実際の条項が適用される範囲はとても広かったので、上記の目的を達成する過程で、保護されるべき表現を大量に取り除いてしまう可能性があった。上記のうち2つの議案は最終的に大きな論争を生み出した。これらの議案は表現の自由及びインターネット一般の自由への脅威と受け取られたため、インターネット活動家、テクノロジー会社及び一般公衆により広く反対された[92]。実際、SOPA及びPIPAへの抗議は、言論の自由の権利

---

[89] S. 3804, 111th Cong. (2010), *archived at* http://perma.cc/EQ5S-2B28.

[90] H.R. 3261, 112th Cong. (2011), *archived at* http://pcrma.cc/88NK-M47F.

[91] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. (as amended, May 26, 2011) [hereinafter PIPA], *archived at* http://perma.cc/LK8N-9PB4.

[92] SOPA及びPIPAへの抗議の歴史について、see generally EDWARD LEE, THE FIGHT FOR THE FUTURE (2013), *archived at* http://perma.cc/6CNV-F7E3. 論争が高まる中、2012年1月18日、Wikipediaは2つの法案に抗議するためブラックアウトし、Googleは詳しい情報へのリンクとともに反SOPAロゴを用い、Mozillaは Mozilla.org及びMozilla.comの英語の各ウェブサイトを訪れると “action page” に移動するようにし

の防御における、人々の支持を得た立憲主義の最も有名な最近の事例の 1 つである[93]。

これらの議案は法として制定されなかったが、2 つの理由により示唆に富んでいる。まず、コンテンツ業界による継続的なロビイング活動を受ける議会は、将来同様の立法を試みる可能性が十分にある。第二に、これらの議案は、政府がその気になれば、多くの異なるデジタルインフラストラクチャーの側面を、新しい巧妙なコントロールの手法にいかに利用することができるかを示している。それゆえ、SOPA、PIPA、及び COICA において用いられたテクニックを学ぶことは、私たちに、将来あり得る自由言論に関する紛争への窓口となる。

例えば、SOPA の Section 102 は、アメリカ合衆国司法長官に、「海外の侵害サイト」に対して差止めを得る権限を与えていた[94]。この用語は、ドメインネームがアメリカ合衆国外で登録されたサイトを含むよう（サイトを保有しているアメリカの会社が海外の登録機関を使っている場合を含むよう）、広く定義されていた[95]。より重要なこととして、もしサイトのどの部分かが著作権侵害を「助長する」場合は、サイトは「侵害する」もの

た。Vlad Savov, *The SOPA Blackout: Wikipedia, Reddit, Mozilla, Google, and Many Others Protest Proposed Law*, THE VERGE (Jan. 18, 2012, 12:10 AM), http://www.theverge.com/2012/1/18/2715300/sopa-blackout-wikipedia-reddit-mozilla-google-protest, *archived at* http://perma.cc/GVK3-9DFM; *see also* Yochai Benkler et al., *Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate* (Berkman Ctr. for Internet & Soc'y, Research Publ'n No. 2013-16, 2013), *archived at* http://pcrma.cc/5SB4-YYJK（オンライン上の論争の発展を示す）.

93 裁判所が 2 つの議案の合憲性を認めなかったため、このエピソードは、アメリカ合衆国における表現の自由の概念を形作った多くの政治的論争と同じ範疇に属する。*See generally* MICHAEL KENT CURTIS, FREE SPEECH, "THE PEOPLE'S DARLING PRIVILEGE" (2000)（アメリカの歴史における言論の自由の重要な論争について検討している）.

94 H.R. 3261 § 102.

95 *Id.* § 101(4), (8). *See* Marvin Ammori, *SOPA/PIPA Copyright Bills Also Target American Sites*, AMMORI.ORG (Dec. 31, 2011), http://ammori.org/2011/12/31/sopapipa-copyright-bills-also-target-domestic-sites/, *archived at* http://perma.cc/5UBX-7UXB（Google.ca 及び Amazon.co.uk の例を挙げる）.

として扱われていた[96]。「助長する」との文言は曖昧で、様々な解釈の余地がある。それは、顧客がしばしば侵害的なコンテンツをアップロードしたり、そのようなコンテンツにリンクを貼ったりする、例えばFacebookやYoutubeのようなプラットフォームに適用される可能性があった。もしこれらのサイトが当該コンテンツをブロックするフィルターをインストールしていなかったり、アップロードされることを防止していなかったりすれば、例えそれらのサイトが特定の侵害行為を知らず、既存の著作権法の下で二次的な責任ありとされなくとも、それらは法的な意味において「侵害を助長する」とされるかもしれなかった。

したがって、Section 102は、DMCAのセーフハーバールールを上手くかわすことをもって媒体を脅かすものであった。すなわち、DMCAのセーフハーバールールは、媒体が実際に彼らのサービス上の侵害行為を知っていたか、又はDMCAの下院におけるレポートの文言によれば「明らかな侵害の『目印』に目を閉ざしていた」場合でない限り、著作権侵害の責任から媒体を保護していたのである[97]。

DMCAの実際の認識に基づく基準は付随的検閲の問題を緩和した。逆に、Section 102は法律上の定義に当てはまる媒体に、例えばコンテンツフィルターをインストールすることを通して、コンテンツ産業の利益になるであろう付随的検閲に従事する動機を与えたであろう。このように、アメリカ合衆国でビジネスを行っている当事者に対する差止めの目的は、その活動を停止させることではなく、その者を他の者のコンテンツや言論のフィルタリングとブロッキングに従事するように仕向けることである。換言すると、差止めの目的は付随的検閲である。

(d) デジタルインフラストラクチャーに向けられる事前抑制―しかし、多くの場合、「海外の侵害サイト」であるとされるサイトはアメリカ合衆国の国外にあり、アメリカの裁判所の管轄に服さないであろう。そのような事例においては、合衆国検察官は反対当事者の審問を経ずに差止めを得

---

[96] H.R. 3261 § 102(a).

[97] H.R. REP. No. 105-551, pt. 2, at 57 (1998); *see also* 17 U.S.C. § 512(c)(I)(A)(ii)(2012)（セーフハーバーの恩恵を受けるためには、ISPは「侵害行為を明白に示す状況又は事実を認識していてはならない」と規定する）.

ることができた[98]。もちろん、当該海外サイトに向けられた差止めはサイトそれ自体を停止させるためにはあまり意味がない可能性がある。しかし、一たび検察官が一方当事者のみに対する審問による手続を許されると、この法律の本当の効果が明らかになる。大元のサイトを追う代わりに、検察官はアメリカ合衆国内の多くの異なったデジタルインフラストラクチャーの担い手に命令を発することができるであろう。すなわち、政府はサーチエンジンに対しそのサイトにリンクをしないように命令することができ、オンライン広告社にそのサイト上で広告を行わないように命じることができ、また決済業者（クレジットカード会社など）にアメリカの顧客とそのサイトの間のビジネスを扱わないように命じることができる[99]。

おそらく最も重要なこととして、検察官はブロードバンド通信会社、大学のネットワーク、図書館、私的ネットワーク、電話会社及びケーブル会社を含む全てのインターネット「サービスプロバイダ」[100]に対し、「アクセスを防ぐための技術的に実行可能で合理的な手段」をとるように命じることができた[101]。これはブロッキングやフィルタリングを行うことだけではなく、サイトのドメインネーム（例えばnytimes.com）がドメインに割り当てられたインターネットプロトコルアドレス（例えばnytimes.comに現在割り当てられている170. 149. 172. 130[102]）に還元することを禁止することを含む。言い換えると、政府は、馴染みのあるドメインネームをネットワーク間のコミュニケーションを可能とする数字のインターネットアドレスへと翻訳する、ドメインネームシステムの実際の働きを妨げる命令を出すことができた。このドメインネームシステムが正常に機能することは、世界規模の効果的なコミュニケーションだけではなく、サイバーセキュリ

---

98 *See* H.R. 3261 § 102(b)(2).

99 *Id.* § 102(C).

100 *Id.* § 102(c)(2)(A); *id.* § 101(22)(cross-referencing 17 U.S.C. § 512(k)(I)(2012)).

101 *Id.* § 102(C)(2)(A).

102 *See IP Locator Also Known as IP Lookup Tool*, IP TRACKER, http://www.iptracker.org/locator/ip-lookup.php?ip=nytimes.com, *archived at* http://perma.cc/5YDL-R7BG (last visited May 10, 2014)（nytimes.comのIPアドレスを特定する）.

ティにとっても重要である[103]。

上記全ての事業者は、命令に反対した場合には政府との訴訟に直面する可能性があったが、協力した場合は法的免責を受けた[104]。したがって、SOPAは、政府が侵害的な素材を含む海外サイトの割合（1,000頁の中の1頁だけということもあり得る）や、素材が実際に侵害的であることを証明したかどうかにかかわらず、インターネットインフラストラクチャーの重要な担い手に対し、全てを一方当事者に対する審問による手続で、アメリカ市民による海外サイトへのアクセスをブロックすることを助けるインセンティブを作り出した。このテクニックは、政府に、元の出版者に対してではなく、デジタルインフラストラクチャーの重要な側面に対するコントロールを与える限度において、伝統的な事前抑制よりも強力なものとなり得る。

(e) デジタルインフラストラクチャーに向けられた「私的事前抑制」―第三者に対する政府命令に加え、SOPAのSection 103は「私的事前抑制」とも言うべきデジタルコントロールの新しい仕組みを定めていた。それは私人をデジタルインフラストラクチャーを運営する他の私人をコントロールする代理人とした。もし私人がオンライン広告業者又は決済業者に対し、その者が「アメリカの財産の窃取（theft）に用いられている」[105]ウェブサイトとビジネスを行っていると知らせた場合、その広告業者と決済業者は、当該サイトと取引することを5日以内に止めない限り、法的制裁に直面する可能性があった[106]。請求者である私人は、実際にこの装置を働かせ

---

[103] *See* Mark Lemley, David S. Levine & David G. Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34, 34-35 (2011)（SOPA及びPIPAのDNS規定の効果を論じる）; Vint Cerf et al., An Open Letter from Internet Engineers to the United States Congress (Dec. 15, 2011), *archived at* http://perma.cc/32MP-LUAZ（SOPA及びPIPAは深刻なセキュリティリスクを生むであろうと論ずる）.

[104] H.R. 3261 § 102(C)(5).

[105] *Id.* § 103(a)(I)（引用符を省略）.

[106] *Id.* § 103(b); *Id.* § 103(d)(4). 疑われたサイトがカウンターノーティスを出した場合、*Id.* § 103(b)(5), 又は決済業者又は広告業者が5日以内に当該サイトとビジネスを行うことを止めなかった場合、*Id.*§ 103(c), 訴えた者は、ドメインネームの登録を防ぐためにドメインネーム登録者に対し差止めを求めて訴えることもできる。*Id*.

るために何かを裁判所で証明する必要はなかった。すなわち、サイト又はその一部分（数千ページにより構成されるウェブプラットフォームのうちの１頁でもよい）の活動により害を受けているとの訴えを行うのみでよかった[107]。

「アメリカの財産の窃取（theft）に用いられる」との用語も非常に広く定義されていた。それは、その事業者が特定の侵害行為を知っていたか、また既存の法の下で二次的に責任を負うかにかかわらず、その事業者が侵害を「促す」[108]か、そのサイトでの侵害行為の「高い蓋然性を確認することを避けた」[109]場合を含んでいた[110]。この規定は、表現の自由のデジタルインフラストラクチャーの重要な集合体と言うべき、ユーザーに制作されたコンテンツに依拠するビジネスのほとんどを脆いものとした。第三者が決済業者及び広告業者をそのようなビジネスを営む会社と取引することから遠ざけるよう継続的に脅すことができた。

私的事前抑制の要点は、広告と決済システムに依拠するビジネスにフィルターをインストールさせ、継続的に警戒に当たらせ、そのプラットフォーム又はウェブサイトの一部にある疑わしいコンテンツを取り除かせるように仕向けることにある。換言すると、システムの目的は、各会社を付随的検閲に従事するように仕向け、行き過ぎたフィルタリングとブロッキングという、予想どおりの結末を導くことである。拒否した会社は、取引を続けてくれる決済業者と広告業者を急いで探す必要がある。その会社と取引する者がいない限り、その会社の運営はその分だけ縮小される。この特徴は、次のテクニックの組み合わせであるデジタルブラックリストに繋がる。

C．公的並びに私的協働及び引込み―マッカーシズムからデジタルブラックリストへ

１．従来型の規制：公的並びに私的協働及び引込み―従来型の規制においては、国家は単独では行為を行わない。私人は言論を規制するよう国家

---

107 *Id.* § 103(a)(2).

108 *Id.* § 103(a)(I)(B)(i).

109 *Id.* § 103(a)(I)(B)(ii).

110 *See supra* p. 2313（DMCAにおける意図の基準を論ずる）.

を後押しすることができ、援助することを申し出ることさえできる。逆に、国家はアメかムチかあるいはその両方を通じて私人の協力を求めることができる。関連する戦略はメディア協働である。出版社は政府の役人との関係を良好に保ち、また政府ソースへの継続的なアクセスを持つことを切望するので、メディア組織は、報道を取り止め、報道を歪曲し、自己検閲し、また厄介な素材の出版を遅らせることに導かれる可能性がある。

私人はまた私的監視に従事し、疑わしい人々を当局に示し、国家への反対者や国家が制限したがる活動に関与していると疑われる人物を遠ざけ、又はそのような者との取引を拒絶することにより、国家を助けることができる。今日私たちがMcCarthy期と連想するブラックリストシステムは公的・私的な協働・引込みの具体例である。すなわち、政府は、産業、教育、芸術、及び専門職の中の共産主義者を見付け出したいという欲求を明らかにした。民間の企業及び人々は、これを、政府による転覆活動家の捜索に協力することを拒んだ人々、又は政府の転覆に共感を持つと思われる人々とビジネスをすることを拒むように、とのメッセージとして受け取った。

2．最新型：データ共有、免責及びデジタルブラックリスト―公権力と私人の協力と協働の選択は、最新型の言論規制の顕著な特徴である。[111] 政府は、最近明らかになった政府による監視においてそうだったように、あるときは私的インフラストラクチャーの所有者に対し、監視の仕組みについて口外することを禁止する報道禁止命令（gag orders）を出す。[112] また、あるときは、政府はアメとムチとを使い分ける。その最も重要なものは、政府が気に入らないインターネットサイトや発言者（speaker）を特定し、シャットダウンさせることを手助けすることと引き換えに、法的な免責を認めるものである。

(a) データへのアクセス―多くの民間事業者が、監視や分析を促進するために個人データを収集し、そのデータを政府に販売する。このようなプ

[111] *See generally* Yochai Benkler, *WikiLeaks and the PROTECT-IP Act: A New Public-Private Threat to the Internet Commons*, DAEDALUS, Fall 2011, at 154; Michael D. Birnback & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003).

[112] *See infra* Part III, pp. 2329-40.

ラクティスによって、連邦・州政府は、修正第4条の要件を迂回することができる。[113] 私企業―通信事業者、検索エンジン、ソーシャルメディア企業を含む―は、自ら又は媒体を通じて、保有するデータへのアクセスを、進んで行うかどうかは別として、許すことができる。私企業はまた、[114] 政府の要求（又は強制）により、その通信やデータ保存システムに政府の監視を可能にする特別なアクセス用の設備又は「バックドア」（裏口）を設けることができる。[115] 更に、国は、協力、技術上のアクセスの見返りとして、又は政府が害をなす若しくは危険であると判断する表現を監視しブロックする見返りとして、私企業に対して免責を提供することができる。例えば、2008年のFISA改正法[116]は、政府とデータを共有する見返りに、通信事業者に遡及的な免責を提供した。[117] 逆に、協力しないと、法的な責任又は規制圧力に晒される可能性がある。

(b) 付随的な検閲に対する免責―国は、媒体が付随的な検閲を行う場合に免責を付与することができる。仮に媒体が望ましくないコンテンツを検索し、ブロックし、又はそれを発行した関係当事者と取引することを拒絶しても、法的には責任を負わない。しかしその媒体がそうした検索・ブロック・取引拒絶を怠ると、違法コンテンツについて、寄与侵害又は代行侵害の責任を負うことになる。

SOPAのSection 103は、こうしたテクニックの一例を示している。ある

---

[113] *See* ROBERT O'HARROW, JR., NO PLACE TO HIDE 2–4 (2005)（法執行機関が利用できる様々なデータ収集（aggregator）サービスを説明する）.

[114] *See* Joshua Brustein, *Tech Giants, Like Telecoms, Have Been Sharing with the NSA*, BLOOMBERG BUSINESSWEEK (June 6, 2013), http://www.businessweek.com/articles/2013-06-06/tech-giants-like-telecoms-have-been-sharing-with-the-nsa, *archived at* http://perma.cc/FWF6-JLYS.

[115] Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 6, 2013, at A1.

[116] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. §§ 1812, 1881, 1881a–1881g, 1885, 1885a–1885c (2006 & Supp. V 2011)).

[117] *See id.* § 201, 122 Stat. at 2468–70（§ 802を追加、現在は、50 U.S.C. § 1885aとしてFISAに法制化された）.

決済業者又は広告業者が、別の私人から、当該決済業者又は広告業者が法律の適用対象となるサイトと取引を行っているとの通知を受けた場合、当該決済業者及び広告業者は、そのサイトとの取引を拒絶すれば、例えそうした申立てが裁判所において証明されたものではないとしても免責される。[118] この法律の前身の法案であるCOICAは、私人に対してよりストレートに協力を推奨するものであった。[119] COICAは、司法長官に対して、「情報と合理的な確信に基づき違法活動に利用されていると判断されるが、司法長官が本項に基づく訴訟を提起していないサイトの公的なブラックリストを作成する」[120] ことを要求していた。あるサイトが司法長官リストに掲載されると、インターネットサービスプロバイダ（ISPs）、決済システム提供者、ドメインネームサービス提供者及び広告業者がそのサイトとの取引を停止し、又はサービスの供給を拒否しても免責される。[121] その際、司法長官リストに掲載されていないことを証明する責任は、サイト側に課される。[122] この精巧な私的事前抑制のシステムは、政府の公的な認可システムや裁判上の差止めを必要とすることなく、伝統的な事前抑制のコストと立証責任の転換の全てを達成する。COICAの次のバージョンは、司法省のブラックリストに代え、制定法によって私的なブラックリストに対し根拠を与えた。「ドメインネームレジストリ、ドメインネームレジストラー、金融取引業者又はインターネットサイトに対して広告を提供するサービス業者は、インターネットサイトが侵害活動に利用されていると合理的に考える場合…、本項に記載された措置を第三者に対して自発的に講じても、責任を負わないものとする。」[123]

知的財産保護法（PROTECT IP Act）のSection 5は、同様に、「決済業者

---

[118] Stop Online Piracy Act, H.R. 3261, 112th Cong. § 103 (2011).

[119] *See* Benkler, *supra* note 111 , at 160–61.

[120] Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. § 2324(j)(1) (2010) (as referred to S. Comm. on the Judiciary, Sept. 20, 2010).

[121] *See id.* § 2324(j)(2).

[122] *See id.* § 2324(j)(3).

[123] Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. § 2(e)(5)(B) (2010) (as reported by the S. Comm. on the Judiciary, Nov. 18, 2010).

又は広告業者が善意に、かつ信頼できる証拠に基づきインターネットサイトが違法活動に利用されていると合理的に考える場合、当該インターネットサイト」との取引を自発的に拒絶することについて法的責任を免除している。[124] こうした免責規定のポイントは、業界におけるブラックリストの作成を促すこと、そして、例えブラックリストに誤った情報が含まれていたとしても、そのリストを作成したこと及びそれに基づいて行動したことについて免責されることである。

（c）ソフトパワー―また、政府関係者は、非公式に表現規制を促すことができる。[125] 我々は、こうした技術を付随的検閲の法の枠を超えた方法と理解することができるだろう。最近の最も顕著な例は、民間企業に対して直接の命令や脅威を与えることなくWikiLeaksを閉鎖させようと試みたアメリカ政府の行動である。[126] 2010年11月28日、WikiLeaksとそのマスメディアのパートナー― *Guardian*, *New York Times*, *Der Spiegel* といった著名な組織―は、世界中のアメリカ大使館とアメリカ合衆国国務省の間のその数約25万に上る機密通信の中から文書を開示し始めた。[127] 政府機関や政治家の反応は素早く、またそれらの反応は伝統的なマスメディアのパートナーではなく、WikiLeaksに対して直接向けられた。*New York Times* も機密文書

---

[124] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. § 5(a)（2011年５月26日、上院司法委員会によって報告された）.

[125] *See* Derek E. Bambauer, *The New American Way of Censorship*, ARIZ. ATT'Y, Mar. 2013, at 32, 34, 36–37（間接的又は他の者に対する影響を通じてその目標を達成する「ソフトセンサーシップ」の複数のツールを論じる）. Bambauerは「ソフトセンサーシップ」を私の言う「ソフトパワー」より幾分広く定義する。「ソフトセンサーシップ」は、「素材をブロックするための序文として無関係の法律を用いること、アクセスをフィルタリングするために支払いを行うこと、又は媒体にコンテンツを制限するように説得することを含む。」Bambauer, *supra* note 8, at 867.

[126] *See* Bambauer, *supra* note 8, at 891–93（WikiLeaksにプレッシャーをかけるための多方面からのキャンペーンについて述べる）; Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 330–51 (2011) (same).

[127] Benkler, *supra* note 126, at 326.

を共同して公表した当事者であったが、副大統領Joseph Bidenは、WikiLeaksの設立者Julian Assangeは、「Pentagon Papersではなく、ハイテクのテロリストに近い」と論じ、[128] 国防省長官のHillary Clintonは、外交通信の公開を「国際社会への攻撃」[129]と呼んだ。

2010年11月27日、通信の公表が始まる前日、アメリカ合衆国国務省の法務アドバイザーHarold Kohは、WikiLeaksに対し巧妙に書かれたレターを送付し、それは一般に回覧された。[130] その中では、WikiLeaksが機密文書を公表することにより法律違反を犯した若しくは犯そうとしている、又はWikiLeaksやそのパートナーの活動が憲法上保護されないといったことは、直接は指摘されていない。[131] その代わり、そのレターは、誰が法律に違反したかについては言及することなく、開示された素材が「米国法に違反して提供された」と断定した。[132] そのレターは、「WikiLeaksがその素材を保有する限り、違法状態は継続する」と述べ、そして、「WikiLeaksは、25万の文書を出版するために*New York Times*、*Guardian*及び*Der Spiegel*に提供し、機密文書の違法な拡散を更に行っている」と指摘した。[133] このように、国防省は、直接的にはWikiLeaks自身が法を破ったとは主張していないが（*New York Times*が破ったとも示唆する）、「（何者かによって）違法行為があったことを正確に認め、WikiLeaksがその違法行為の当事者であることを示唆した」。[134]

---

[128] *Julian Assange Like a Hi-Tech Terrorist, Says Joe Biden*, THE GUARDIAN (Dec. 19, 2010, 1:20 PM), http://www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden, *archived at* http://perma.cc/56HV-MKF7.

[129] Glenn Kessler, *Clinton, in Kazakhstan for Summit, Will Face Leaders Unhappy over WikiLeaks Cables*, WASH. POST (Nov. 30, 2010, 8:44 AM), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/30/AR2010113001095.html, *archived at* http://perma.cc/4VUE-6KJ7.

[130] Letter from Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, to Jennifer Robinson, Attorney for Julian Assange (Nov. 27, 2010), *archived at* http://perma.cc/653P-2LZF.

[131] *See id.*

[132] *Id.*

[133] *Id.*

[134] Benkler, *supra* note 111, at 156

12月１日、上院国家安全保障委員会の委員長であるJoseph Lieberman上院議員は、民間企業に対してWikiLeaksと取引を行わないよう求めた。[135] 彼の事務所は、WikiLeaksをサーバー上に置いていたAmazon.comに対し、WikiLeaksとの関係を質すため私的に連絡をとった。[136]

国務省の公開レターとLieberman上院議員の公開要求に続き、デジタルインフラストラクチャーの様々な部分がWikiLeaksに対するサービスを拒否し始めた。Amazonは、即座にWikiLeaksをサーバーから取り除いた。[137] WikiLeaksのドメインに利用されていたドメインレジストラーであるEveryDNSは、WikiLeaks.orgがWikiLeaksサーバーを指し示すことを止めた。[138] PayPalは、国務省のレターに基づき、WikiLeaksに対する支払いを取り扱うことを止めた。[139] Visa、MasterCard及びBank of Americaも間もなくそれに加わった。[140] その月の後半には、iPadとiPhoneにダウンロードできるアプリケーションを管理するAppleが、iPhoneユーザーにWikiLeaksの外交文書へのアクセスを可能にする第三者作成のアプリケーションをApp Storeから排除した。[141] WikiLeaksは、代わりのサーバーホスティング及びストレージとスイスのドメインネームを見付けることができたが、決済サービスを失ったことは、サービスを継続する能力にダメージを与えた。[142]

WikiLeaksのエピソードは、政府が、明瞭か否かを問わず、また何らかの脅威を与えることなく、単にデジタルインフラストラクチャーの管理者

---

[135] Charles Arthur, *WikiLeaks Under Attack: The Definitive Timeline*, THE GUARDIAN (Jan. 8, 2010, 11:39 AM), http://www.theguardian.com/media/2010/dec/07/wikileaks-under-attack-definitive-timeline, *archived at* http://perma.cc/E6B2-XHSY.

[136] Rachel Slajda, *How Lieberman Got Amazon to Drop Wikileaks*, TALKING POINTS MEMO (Dec. 1, 2010, 9:56 PM), http://talkingpointsmemo.com/muckraker/how-lieberman-got-amazon-to-drop-wikileaks, *archived at* http://perma.cc/YV55-JCQS.

[137] Benkler, *supra* note 126, at 339–40.

[138] *Id.* at 340.

[139] *Id.* at 341.

[140] *Id.* at 341–42.

[141] Benkler, *supra note* 111, at 157.

[142] *Id.* at 157–58.

である私人に対して権利侵害する表現者を止めるよう促すことにより、いかに表現の自由のインフラストラクチャーの私的なコントロールを利用できるかを示している。[143] WikiLeaksの立ち位置は、*Pentagon Papers*事件での*New York Times*のそれとほとんど変わらなかった。すなわち、WikiLeaksは1つのソースから大量の素材を受領し、それを世界に向けて公表した。しかし、アメリカの政府当局にとって、公的な声明とよく狙い澄ました依頼というソフトパワーを用い、表現の自由のデジタルインフラストラクチャーをコントロールする民間企業に対してWikiLeaksとの取引を停止するように説得することは驚くほど簡単なことであった。その理由の1つは、多くの企業が悪い評判を嫌い、良い企業市民であると思われることを好むことにある。彼らは、不当に政府に干渉されることなく利益を上げ、また顧客の大多数に奉仕する静かな生活を好んでいる。また、もう1つの理由は、WikiLeaksがそのパートナーである伝統的なメディアとは異なって概ね無名の事業体であり、容易にその評判は悪化し、犯罪者又はテロリスト集団であると描かれたことにある。とりわけ、オバマ政権とLieberman上院議員は、*Guardian*、*Der Spiegel*はもとより、*New York Times*に対しても同様の対応をとらなかった。もし、公にVisa、MasterCard及びAmazonに対して*New York Times*との取引を控えるよう促していたら、それは報道の自由に対する重大な侵害であり、デジタルマッカーシズムの新しい一形態になっていたであろう。

Ⅲ．デジタル監視を手助けする事前抑制：国家安全文書

監視が表現の自由と結社の自由にどのような方法で影響を及ぼすかについての網羅的な議論を展開することは、この論文の範囲を超えている。[144]

---

[143] *See* Bambauer, *supra* note 8, at 894–99（政府がインフラストラクチャーを担う会社に対して言論を制限するように促し、説得し、丸めこむための複数のテクニックを説明する）.

[144] *See, e.g.*, Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

本稿で私が関心を持っているのは、より特定された問い、すなわち、デジタル監視の需要がかつてないほど高まっていることが、政府が表現の自由のインフラストラクチャーを標的にすることにどのように繋がっているか、である。

デジタル時代は、通信とコンテンツ制作の民主化だけでなく、デジタル監視の広がりと、私が他で「国家的監視国（the National Surveillance State）」と呼ぶ国家の監視能力の拡大をもたらした。[145] しかし、政府は、監視を行うためにほとんどの人々が会話に利用する設備に対してアクセスする必要がある。そのため、大部分が民間によって担われている表現の自由のインフラストラクチャーにアクセスする必要がある。こうして、国家的監視国の支配が要求するため、表現の自由のインフラストラクチャーを所有する私人に対し、政府の監視活動を支援することを強制する又はそうした支援に引き込む必要が生じる。そうした協力は新しいものではない。前デジタル時代、通信事業者は、しばしば、政府の監視の努力を支援した。[146] しかし、監視の需要と可能性は急激な高まりを見せており、またデジタル時代における会話のほとんどは、民間で所有されているデジタルネットワーク、サービス、又はプラットフォームを通じてなされているため、デジタル監視には、官民の協力がかなりの程度必要とされる。

逆に、官民の協力の必要性は、民間企業に対し、そうした協力の性質と程度を公開しないことを求める。すなわち、多くの場合、民間のインフラ

---

[145] *See* Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3 (2008); Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006).

[146] 例えば、Project SHAMROCKを通じ、電信会社はNSAに「1945年８月から1975年５月の間に合衆国から発せられた国際電信のほとんどを提供した。」S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK III: SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 765 (1976); *see also* L. Britt Snider, *Unlucky SHAMROCK: Recollections from the Church Committee's Investigation of NSA*, STUD. INTELLIGENCE, Winter 1999–2000, at 43, *archived at* http://perma.cc/VTN9-JVVJ.

ストラクチャーの所有者が政府の監視の内容を明らかにすれば、監視の事実をほのめかし、監視を無駄にすることになってしまう。それゆえ、政府によるデジタル監視プログラムは、必然的に民間のインフラストラクチャー所有者に対する事前抑制、又は事前抑制と同様に働く技術に辿り着く。デジタル監視が広く行き渡るということは、事前抑制が広く行き渡ることと表裏一体なのである。

デジタル監視が広範な事前抑制の利用を必要とする良い例は、政府による国家安全保障文書（「NSL」）の発行である。2001年の米国愛国者法は、多くの様々な政府機関にテロと外国諜報機関の調査にNSLを利用することを許し、NSLの利用はこれにより急増した。NSLの利用は2つの中核的な特徴を持っている。1つは、裁判所の令状や審問を経ずに行政庁職員によって発行できることである。[147] もう1つは、通常、NSLの発行の際に報道禁止命令（a gag order）が伴うことである。[148] NSLの受領者は、NSLの内容やその存在を公表することが許されておらず、政府が公開するまで報道禁止命令に服することになるが、結局政府が公開しない可能性もある。[149]

---

[147] *See* 18 U.S.C. § 2709(b) (2012)（FBIのディレクター、その他の公務員が、電気通信サービス事業者に対して利用者に関する特定の情報を求める権限を付与する); *id.* § 2709(a)（電気通信事業者に対し、NSLの内容を遵守することを義務付ける).

[148] FBI高官が、「アメリカの国家の安全に対する危険又は、犯罪捜査・反テロリズム・反諜報活動のための捜査妨害、外交関係に対する障害、人の生命身体の安全への危険が生じる」と認める場合、（NSLの）受領者は、受領の事実又はその内容若しくは付随する報道禁止命令を第三者（代理人である弁護士を除く）に対して開示することができない。*Id.* § 2709(c)(1). 政府は、NSLの97％に報道禁止命令が付されていると算出している。*In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1074 (N.D. Cal. 2013).

[149] 18 U.S.C. § 2709(c)(1). 政府はまた、愛国者法215条に基づき、通信事業者に対し電話の大量のメタデータを提供するよう求める際に報道禁止命令を用いる。*See* 50 U.S.C. § 1861(c)(2)(E) (2006 & Supp. V 2011); *id.* § 1861(d)(1). 215条の命令は、外国諜報活動監視裁判所又は事後手続で指定された判事より取得される。*Id.* § 1861(b)(1). 215条の非開示命令は、発行されてから1年経過後にのみ異議を申し立てることが許される。*See id.* § 1861(f)(2)(A)(i).

また、非開示命令は外国諜報活動監視法の702条に基づいても発せられる。*See* 50 U.S.C. § 1881a(h)(1)(A) (2006 & Supp. V 2011)（司法長官による命令が正当化され

2006年の愛国者法の再承認前は、裁判所でNSLに異議を申し立て、報道禁止命令の撤回を求めることは不可能であった。[150] 愛国者法の再承認の際、議会はNSLに対する限られた司法審査を付け加えた。[151] この変化は理論的には救済の可能性をもたらすものだが、政府の同意なく報道禁止命令を撤回することが非常に難しくなるよう意図的に設計されている。[152]

る); *id.* § 1881b(c)(5)(b)（海外にいる米国人に関する事案において裁判所の非開示命令を正当化する). 通信事業者は、受領したらすぐに1881条ａに基づき、命令に異議申し立てできる。*Id.* § 1881a(h)(4)(A).

次に、NSLに焦点を当てる。なぜなら、それが表現の自由にとって最も厄介な状況を作っているからである。215条及び702条の命令とは異なり、NSLの非開示命令は事前の裁判所による審問なく強制されるからである。にもかかわらず、同様の難点の多くが215条や702条に基づく非開示命令にも当てはまるのは、それらの命令も一方当事者だけが出席する形で発せられ、（更に）215条の場合には、双方審尋の形で裁判所に再考を促す機会もすぐには付与されないからである。

[150] *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 115, 116(a), 120 Stat. 192, 211–14 (2006), *amended by* USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, § 4(b), 120 Stat. 278, 280 (2006) (18 U.S.C. § 3511 (2012) に法文化された); John Doe, Inc. v. Mukasey, 549 F.3d 861, 867–68 (2d Cir. 2008)（§ 3511 の追加を説明する).

[151] 18 U.S.C. § 3511(b) (2012).

[152] 18 U.S.C. § 3511(b)(2) は、報道禁止命令を維持しやすくする強い推定を作り、政府が裁判所に対して命令を維持するように求めることを非常に容易なものとしている。同条は、裁判所が「開示により米国の安全に対する脅威、犯罪捜査・反テロリズム・反諜報活動のための捜査妨害、外交関係に対する障害、人の生命身体の安全への危険が生じると判断する場合、裁判所は非開示の要件を修正ないし無視することができる。」しかしながら、政府の高官（例えば、機関の長、司法副長官、連邦捜査局のディレクター）が「開示により米国の安全に危害を生じ、又は外国関係に障害を生む可能性があると認める場合、そのような認証は、そのような判断が悪意を持ってなされたと裁判所が判断しない限り、最終的な判断とされるものとする。」 *Id.*

同様に、18 U.S.C. § 3511(b)(3) は、報道禁止命令を受領した者が元の命令を修正又は除去する権限を非常に制限している。裁判所が命令の撤回を求める申立てを認めない場合、受領者は、再びその修正や撤回を求めるために１年待たなければならない。

NSLは、監視のためのインフラストラクチャーと表現の自由のためのインフラストラクチャーとが一致していることを示す、説得力のある例である。表現の自由のインフラストラクチャーを持たない政府は、民間の所有者に監視を支援させるか又は協働させることを必要とする。また、政府は、民間事業者が政府の活動はもちろん、政府から参加を強制する命令を受領したという事実さえ開示しないようにしなければならない。ある匿名のNSL受領者の言葉では、国家は、その受領者を「政府の諜報員」として駆り出すのである。[153]

報道禁止命令は、民間のインフラストラクチャーの所有者に対して監視の対象を漏えいすることを禁じるだけではなく、一般公衆に政府の監視活動の範囲と内容を知らしめないようにする手助けもしている。この特徴ゆえに、NSLは、社会から警戒されることなく広くデジタル通信の背後に存在するものとして機能している。実際、愛国者法の拡張の最も重要な結果の１つは、NSLを政府による捜査の一般的な特性としたことであった。デジタル監視が官僚機構の中で通常のものとなり、広がっていくにつれて、ますます個別的に判断し、重要な手続保障を与えることが難しくなっている。

監視の標的を特定の利害関係者ではなく、インフラストラクチャーの所有者に定めることは、官僚的かつ日常的という国家的監視国における監視の特徴と調和するものである。ほとんどとまでは言えなくとも、NSLの受領者の多くは大企業である。彼らはNSLと報道禁止命令に異議を申し立てる理由を持たないであろう。まず第一に、彼らが政府と良好な関係を望むからである。

第二の理由は、彼らはおそらく、政府の監視に協力している程度（強制か任意かを問わず）を顧客に知られたくないからである。[154] 実際、スノー

---

[153] *See* Anonymous, *My National Security Letter Gag Order*, WASH. POST (Mar. 23, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html, *archived at* http://perma.cc/JA9J-UY4Y.

[154] *See id.*（「捜査機関のレポートは、全ての大手通信事業者がセンシティブな情報を政府機関と共有することに協力してきたことを示唆している。―少なくとも１つの例では、通信事業者がFBIから求められた以上の情報を提供していた。」）.

デンによる暴露の影響の1つはVerizon、Google、Facebookといった大会社が様々な文脈で政府の監視の試みを積極的に支援していた可能性を曝け出したことである。これは、これらの会社のほとんどにとって不名誉なことであった―特に米国外に大部分の顧客層を有する会社にとっては。

NSLの報道禁止命令は伝統的な行政による事前抑制が持つ特徴を全て備えている。一部、*Near v. Minnesota*事件や*Pentagon Papers*事件における司法上の差止命令よりもより顕著な事前抑制として働く点がある。

第一に、NSLの機密性は、監視の範囲と報道禁止命令の期間の両方において、過剰な広がりを促す。NSLの範囲と必要性、そして報道禁止命令の期間の判断を行うのは行政機関なのである。

第二に、NSLの報道禁止命令は、訴訟における主張責任を強力に移転させるものである。NSLの存在は、政府が許可するまで明らかにすることが許されない。政府は、NSLが全く不必要で違法なものだったり政府部内の調査規則に違反するような場合でさえ、むしろそのような場合に特に、報道禁止命令を解除するインセンティブをほとんど持たない。政府は、汚れた衣類を外で干す理由をほとんど持たないのである。2006年の改正後であっても、NSLの報道禁止命令を排除する司法上の救済は非常に限定的なものにすぎない。[155] 更に、裁判所で報道禁止命令の解除を認めさせることに失敗したNSLの受領者は、再度審理を求めるために丸々1年間待たなければならない。[156]

第三に、NSLは、行政機関の職員によって発行され、報道禁止命令が発せられる前に受領者に対し司法上又は憲法上の保護が与えられることもない。行政機関の職員は、修正第1条に関する懸念ではなく捜査を優先してNSLを発行するかどうかを判断し、その判断が司法審査の対象になる場合は非常に限られる。NSLに対する唯一の制限は、修正第1条で保護された行為を調査すること「のみ」を目的としてNSLを発行することができないという点にすぎない。法律は、政府に対して追加の目的を主張することを求めるだけである。[157]

---

[155] *See supra* note 152.

[156] 18 U.S.C. § 3511(b)(3).

[157] *See* 18 U.S.C. § 2709(b)(1) (2012)（FBIのディレクターが情報を求めることを認め

第四に、報道禁止命令の利用によって、現在稼働しているNSLの広範なシステムが公衆には見えないようになっている。毎年秘密裏に何万ものNSLが発行されており、[158] その実例と結果について一番よく知る者は、それを語ることを禁じられている。2007年のある匿名のNSL受領者[159]の以下の論説は、機密性が強制された結果を如実に表している。

> 報道禁止命令の下で生活することはストレスが多く、現実とは思えないものだ。刑事訴追のおそれの下、私は、私の関与する全てを―私がNSLを受け取ったということそれ自体を含めて―同僚、家族、友人に隠さなければならない。弁護士と会う際、ガールフレンドに、自分がこれからどこへ行き、今までどこにいたのかを語ることができない。私は、彼女が見るかもしれないあらゆる場所から、その事案に関する書面を隠す。顧客や友人が私に対し、NSLの合憲性に異議を述べるかと問えば、私は彼らの目を見て嘘をつかなければならない。[160]

第五に、報道禁止命令は、過剰な検閲と濫用へのインセンティブを作り出す。すでに指摘したとおり、政府は報道禁止命令を解除するインセンティブを持たない。特に、NSLが不必要、濫用的、違法又は自身の内部規則に違反しているような場合にそうである。捜査局の報告書は、機密を保つ

る。「但し、米国籍の者が、合衆国憲法の修正第1条によって保護される活動***のみに***基づき行われるものではないこと」（強調追加））.

[158] *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 120–21 (2007) [hereinafter INSPECTOR GENERAL'S REPORT ON NSLS], *archived at* http://perma.cc/MG9F-KMQZ（2005年、47,000以上のNSLの要求が発行されたことを指摘する）.

[159] その匿名の受領者は、その後、Nicholas Merrillであると判明した。See, Ellen Nakashima, *Plaintiff Who Challenged FBI's National Security Letters Reveals Concerns*, WASH. POST (Aug. 10, 2010), http://www.Washingtonpost.com/wp-dyn/content/article/2010/08/09/AR2010080906252.html, *archived at* http://perma.cc/9WX-LS26.

[160] *My National Security Letter Gag Order*, *supra* note 153.

仕組みが濫用を思い止まらせておらず、NSLの濫用事例が複数存在することを示している。[161]

第六に、NSLの受領者は政府によって選び出され、また特定されている。受領者がNSLの内容はもちろん、その存在を開示した場合、政府の権威が直接挑戦を受けていることになるので、その受領者は、訴追される可能性が非常に高い。政府は、その監視活動に対して民間で不服従が広がることを容認することはできない。もしインフラストラクチャーを所有する会社が定期的にNSLを受領していることを公表したら、その他の会社も励まされ、価値ある情報源が台無しになるであろう。それゆえ政府には、あらゆる点から、機密が保持されるNSLの仕組みを傷付けようとする者がどうなるかという具体例を作り出す理由がある。

現在まで、わずかな連邦地方裁判所と1つの巡回区控訴裁判所が報道禁止命令によって提示される修正第1条の論点に取り組んでいるだけである。[162] 2008年、第二巡回区控訴裁判所は、*John Doe, Inc. v. Mukasey* 事件[163]においてNSLの仕組みに関して複数の憲法上の問題点を見出したが、最終的にはその仕組み全体を無効にはしなかった。その代わり、同裁判所は、いくつかの救済となり得る解釈―そのいくつかは、実際の制定法の条文文言

---

[161] *See* INSPECTOR GENERAL'S REPORT ON NSLS, *supra* note 158, at 122–24; *see also* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006, at 5 (2008), *archived at* http://perma.cc/A6GX-WM5D（「FISA裁判所が、修正第1条の懸念点を示し、同じ捜査における215条に基づく命令に署名することを二度拒絶した後に、FBIは［削除編集（redacted）］についての情報を求めるNSLを発行していた」).

[162] *In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064 (N.D. Cal. 2013); Doe v. Gonzales (*Doe II*), 500 F. Supp. 2d 379 (S.D.N.Y. 2007), *aff'd in part, rev'd in part, and remanded sub. nom.* John Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008); Doe v. Gonzales (*Doe CT*), 386 F. Supp. 2d 66 (D. Conn. 2005), *dismissed as moot*, 449 F.3d 415 (2d Cir. 2006); Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *vacated and remanded sub. nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

[163] 549 F.3d 861. 担当裁判官は特に著名である。Judge Jon O. Newman判事が法廷意見を書き、Guido Calabresi判事とSonia Sotomayor（当時）判事（現最高裁判事）が同意見に賛同した。

とほんのわずかな関係しか有していなかった―を提供し、事案の更なる審理を求めて下級審に差し戻した。[164]

NSL は、最新型の表現規制を取り扱う裁判官が直面する困難を例証している。第二巡回区控訴裁判所は、「非公開要件は、ある意味事前抑制である」[165] と指摘し、またそれによって、重要な公共に関わる問題―政府によって秘密裏に行われている監視の程度と濫用に関する公の議論が妨げられると指摘した。[166] それにもかかわらず、裁判所は、Stewart 最高裁判事の *Pentagon Papers* テスト、すなわち、NSL の開示が「直接的で、即時性のある、回復不能な損害を国家又は国民に対して確実にもたらすか」を問うテスト[167]を適用しようとしなかった。政府は、この基準の下では、会社に送達する毎年何万もの NSL に関して勝訴することができなかったであろう。仮に政府がその基準を満たそうと試みたとしても、この立証の必要性に関する審査だけで、各連邦裁判所の事件数の相当の部分を占めることになるであろう。

また、第二巡回区控訴裁判所は、裁判前の報道禁止命令を事前抑制として却下した *Nebraska Press Ass'n v. Stuart* 判決[168]における、より厳格ではないと言い得る基準を適用することもしなかった。*Nebraska Press* 判決は、せいぜい、連邦裁判所が個別の事案ごとに、報道禁止命令が発せられる「前に」、事前抑制に至らない「他の取り得る手段」[169]を検討することを求める

---

[164] *See id.* at 883–85.

[165] *Id.* at 876.

[166] *Id.* at 878（「匿名企業は、限定的であっても情報の種類を表明することを制限されており、その情報は政府の活動に対する意識的な批判に関係するものである。」）.

[167] *Pentagon Papers*, 403 U.S. 713, 730 (1971)(Stewart, J., concurring). *Near v. Minnesota* 判決に基づく Brennan 判事のテストは類似するものである。*See id.* at 726-27 (Brennan, J., concurring)（制限が許容されるのは、最も極限的な状況に関する「非常に制限的な事案」についてのみであること、すなわち、公表することにより、すでに海上にある輸送の安全を危険ならしめる事情を直接的に生じることが必然的であり、かつ、緊急性がある旨の主張と立証が政府によってなされる場合のみであることを論じている）.

[168] 427 U.S. 539 (1976).

[169] *Id.* at 565.

程度であろうと考えられるが、NSLの非開示ルールはこれも満たさないであろう。

その代わり、第二巡回区控訴裁判所は、NSLの報道禁止命令が*Freedman v. Maryland*判決[170]の憲法上の要件を充足しているか否かを問うた。*Freedman*判決は、映画のわいせつ性に関する検査が完了するまでの間、当該映画の上映をブロックする州の検閲委員会に対する憲法上の制限に関するものであった。*Freedman*判決は、州委員会はできるだけ早く上映を禁止するか否かを判断しなければならないこと、当該禁止を支える差止命令を得るために速やかに裁判手続をとらなければならず、当該映画が保護されないという点についての立証責任は州委員会が負っていること、そして、司法審査の制限は特定された短期間でなければならないことを示した。最後に、迅速な司法判断がなされなければならないとした。[171]

*Freedman*判決を援用することは、第二巡回区控訴裁判所が司法審査の基準を意図的に低くしていたということを意味する。[172] *Freedman*判決は、表現の自由としての価値が低いか、又は修正第1条で全く保護されない対象についての許可制に関するものであった。[173] Brennan最高裁判事が*Pentagon Papers*判決で説明したように、同判決は、「抑圧される対象が修正第1条の保護を受けるものであり、唯一の問題が、それにもかかわらず圧倒的に上回まる国家的利益が存在するために、その発表を一定の期間禁止することが許されるか否か」という場合、適用されるべきではない。[174]

最終的に、第二巡回区控訴裁判所は、NSLの報道禁止命令が*Freedman*判決の基準を満たすことさえ要求しなかった。政府は、このテストもクリアすることができなかっただろう。なぜなら、政府は、発行している何千も

---

[170] 380 U.S. 51 (1965).

[171] *See id.* at 58–60; *accord* Se. Promotions, Ltd. v. Conrad, 420 U.S. 546, 560 (1975).

[172] 事実、政府が要求した監視の性格と内容を前提として、第二巡回区控訴裁判所の裁判官は、厳格な基準が適用されるかどうかについて合意に至ることができなかった。その代わり、担当裁判官は、審査基準にかかわらず結論は同じであるとした。John Doe, Inc. v. Mukasey, 549 F.3d 861, 878 (2d Cir. 2008).

[173] *Pentagon Papers*, 403 U.S. 713, 726 n.* (1971) (Brennan, J., concurring).

[174] *Id.*

のNSL１つ１つに関して裁判官の前にすぐに向かうことができず、また、インターネットサービスプロバイダに対する憲法上十分な手続保障を確保した本案判決を迅速に得ることはできなかったはずだからである。

政府の抗弁は、国家的監視国におけるデジタル事前抑制の現実をさらけ出した。まず、政府は、「仮に2005年だけで４万件以上もあったNSLの要求において、非開示を強制するために訴訟を提起しなければならないとしたら、それは不当な負担を政府に負わせるものである」[175]と説明した。言い換えると、政府は、愛国者法制定後のNSLの中核的な特徴は、それが定型的・行政的・官僚的な監視の仕組みであることだと指摘した。そうした監視は、従来型（前デジタル）の監視・言論規制の方法とは異なり、個々の司法審査を受けにくいものである。*Freedman* 判決は、毎年比較的少数の作品が制作される映画に対処することを意図したもので、監視要求を毎年何万件も発行する官僚的なシステムに対処するものではなかった。*Freedman* 判決の基準を当てはめることによってでさえ、監視と報道禁止命令のシステムは停止されるか大幅に縮小されるかしなければならなかったであろう。

第二に、政府は、「NSLの受領者のほとんどが監視の事実の開示を希望していると考える理由がないから」[176]、個々の報道禁止命令について司法審査を負担する必要はないと主張した。その理由とされたのは、前述したように、NSLの大多数が比較的少数の私的インフラストラクチャーの大きな所有者に対して発行されるところ、これらの企業が世界中に有する顧客は、その企業がアメリカのデジタル監視プログラムにどの程度協力しているかについて興味がないということであった。[177] 外国人のみが標的にされているというアメリカ合衆国政府によるこの表明は、これらの企業の海外

[175] *Mukasey*, 549 F.3d at 879.

[176] *Id.*（被告、控訴人の準備書面を引用する at 33, *Mukasey*, 549 F.3d 861 (No. 07-4943-cv), 2008 WL 6082598）（引用表記を省略）.

[177] *See id.* at 880（「典型的なNSLの受領者は…NSLの受領を明らかにすることにどのような意味でも依拠しないビジネスを行っており、NSLの受領を公表するために裁判所で異議申立手続を開始することについてほとんどインセンティブを有しない。」）.

の顧客にとっては背筋が寒くなるものだろう。おそらく、政府の監視活動に対してイデオロギー的に強い反対意思を持つわずかな起業家―匿名訴訟を開始したNicholas Merrillのような―のみが異議申し立てするだろうが、それは個々に対処され得る。

最終的に、第二巡回区控訴裁判所は、政府が事実上「相互通知手続」[178]を守ると合意する限りにおいて、NSLの報道禁止命令システムを支持した。しかし、どれだけ注意深く検討しても、この「相互通知手続」は、制定法の法文上に根拠を見出すことができないものであった。[179] 第二巡回区控訴裁判所は、「政府は、NSLの各受領者に対して、非開示要求に対する異議申し立てを希望する場合、迅速に、例えば10日以内に政府に対して通知すべきであることを受領者に対して知らせる」ことを提案した。[180] 政府が当該通知を受領した場合、「政府は、一定期間、例えば30日間、非開示要件を維持するための裁判手続をとるための時間を与えられる。そして、当該手続が一定の期間内、例えば60日以内に完了しなければならないとする」。[181] その結果は、「政府が訴訟を開始する負担をほとんど取り除くものであろう（対応して、NSLの受領者に、無数の訴訟の防御のために最小限の負担が課される）」。[182] しかし、仮に第二巡回区控訴裁判所の相互通知提案が*Freedman*判決に沿うものであったとしても、政府はその提案を遵守する

[178] *Id.* at 879（内部の引用表記は省略）.

[179] *Id.* at 883（「政府が非公開についての司法審査を求めることを憲法上必要な義務とするためにNSLの法律を『解釈』又は『修正』することは、裁判所の権限を超えるものだが、…政府は、新たな立法なくそのような義務を前提とすることができるかもしれないと指摘する」）.

[180] *Id.* at 879.

[181] *Id.*

[182] *Id.* 更に第二巡回区控訴裁判所は、3511条(b)(2)及び (b)(3)を、NSLの受領の事実を開示することが安全保障に関する害悪を生む危険を生じるとする正当な理由の証明を政府に課すものとして解釈した。*Id.* at 883. また、同裁判所は、2709条(c)及び3511(b)は、「政府に対して司法審査を求める義務を課さずに非公開を課す限りにおいて違憲であり」、*id.*, 3511条(b)(2)及び(b)(3)は、「公開がアメリカ合衆国の安全保障を脅かし、又は外交関係を妨害するという政府の公式判断が最終的なものであると取り扱われる場合には違憲である」と判断した。*Id.*

ために必要な内規をいまだに発行していない。[183]

第二巡回区控訴裁判所は、「非開示要件がある意味で事前抑制である」ことを認識していたが、[184] それを「典型的な」[185]事前抑制とは見なかった。すなわち、裁判所は「公共の場における表現者、文学作品を頒布する者、映画を公開する者など、通常表現の自由の権利を行使したいと思う者に制

---

[183] *See In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1070–72 (N.D. Cal. 2013)（政府は、相互通知手続を遵守すると述べたが、そのための規則を制定していないことを指摘し、NSLの規定は法文上*Freedman* を遵守しておらず、救済解釈にも従っていないと判断する）. *In re National Security Letter* 事件の第九巡回区控訴裁判所に提出された書面において、政府は、「2009年以来、FBIは、匿名による差止命令を遵守し、匿名の『相互通知』手続を全米で実施していると主張した。」 Government's Opening Brief, *In re* Nat'l Sec. Letter, Nos. 13-15957 & 13-16731 (9th Cir. Jan. 17, 2014), *archived at* http://perma.cc/ZYM6-6XDV.

第二巡回区控訴裁判所の提案に加え、諜報活動と通信技術に関する大統領の検討委員会が、緊急時を除き、裁判所の判断後にはじめてNSLが発行されることを推奨している。RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 26–27, 93–94, 122–23 (2013), *archived at* http://perma.cc/R65B-VCUL. これらの推奨に従えば、発行されるNSLの数は減少するだろうが、手続はいまだ事後的なものである。

Freedman の基準を遵守しようとするために、事後ではない迅速な司法判断が必要となる。更に、検討委員会の推奨の下では、NSLが発行された後にその命令を争うための挙証責任はいまだ受領者の側に課されている。*See id.* at 27（「非開示命令は、その受領者が命令の合法性を争うために弁護士に相談することを禁じるような方法で決して発せられてはならない。」）. しかし、推奨は、政府が180日ごとに報道禁止命令の再承認を得ることを義務付ける。*Id.*

また、検討委員会は、政府が開示が国家の安全を損なうものである蓋然性を証明しない限り、報道禁止命令の受領者が、定期的に受領した命令の数・命令を遵守した数・提供した情報の一般的なカテゴリーごとの情報の主体であるユーザーの数を開示することを認める法律を推奨している。
Id. at 123. これは事前抑制の問題を緩和させるが、完全に解決するものではない。

[184] *Mukasey*, 549 F.3d at 876.

[185] *Id.*

約を課すものではない」と述べた。[186] 同裁判所は、*Pentagon Papers* 判決―*New York Times* 社が一般大衆の知る権利の対象となると考えた政府の活動について情報を公開しようとしたのに対し、政府がこれを妨害しようとした―を事前抑制の典型例（paradigm case）とした。[187]

この説明は、最新型の言論規制の 3 つの特徴を見落としている。まず第一に、デジタル時代には、政府は、個人の表現者や*New York Times* 社のような報道機関の構成員を標的にすることはほとんどない。個人を標的にすることは困難で、非効率で、かつ無駄だからである。表現者は匿名であったり、海外にいたりするかもしれない。また、彼らは、非常に早く表現を発することができるため事前抑制が効かないかもしれない。そうではなく、現在は、政府が民間のインフラストラクチャーの所有者を標的にする可能性の方がずっと高い。なぜなら、監視するためには彼らの協力が必要だからである。SOPA の例で見たように、政府は、その業務を行うために、民間のインフラストラクチャーに対して協働を強く求める。デジタル時代においては、これが事前抑制の大きな機能を果たし得る。

第二に、政府は記者と情報源との接触情報を必要とするため、NSL の秘密命令は報道機関に向けられることがある。*New York Times* 社の行為を差し止める代わりに、政府は、*New York Times* 社が誰に向かって、どの位の時間、またどのような機会に会話しているかを知るための NSL を発行することができる。情報漏えいの更なる調査のためと推測されるが、近時、司法省は、Associated Press 社が保有する電話番号の接触の記録を 2 カ月分取得した。[188] 司法省の行動が明らかになった結果、抗議の声が上がり、政府の諜報活動について大きな議論が巻き起こった。結局、司法省はそのよう

[186] *Id.* 裁判所は、非開示規定は、例え、「非開示要件が情報のカテゴリー、…NSL の受領事実とその他関連する細部の事実に基づくものであっても」、「典型的な内容規制」ではないとも付け加えた。*Id.*

[187] *See id.* at 882（*Pentagon Papers* を引用、403 U.S. 713 (1971)（裁判官全員一致））.

[188] *See* Mark Sherman, *Gov't Obtains Wide AP Phone Records in Probe*, ASSOCIATED PRESS (May 13, 2013, 10:53 PM), http://bigstory.ap.org/article/govt-obtains-wide-ap-phone-records-probe, *archived at* http://perma.cc/Y65X-YEZ8.

な請求をするための内部手続を変更することになった。[189] 情報があらわになったのは、司法省が大陪審による召喚状請求手続を利用したためであった。すなわち、司法省の内規によれば、そのような請求は請求から90日以内に公表されなければならない。[190] しかし、もし政府がNSLを利用していたら、電話番号記録の請求の事実は、いまだに秘密にされていただろう。[191]

第三に、そしておそらく最も重要な点だが、民間のインフラストラクチャー所有者は、21世紀の「報道機関」である。合衆国憲法の報道条項における「報道」は、ジャーナリズムの組織体と情報を拡散するために用いられる技術の双方を意味する。[192] 植民地時代、多くの印刷機所有者は、自身の言論のみではなく、その顧客の言論も印刷していた。[193] 政府がISP、ブロードバンド提供事業者やその他類似する事業者を標的にする際、それは、技術的には現代における「報道機関」と同等の存在を標的にしているので

---

[189] Scott Neuman, *Justice Tightens Guidelines for Obtaining Records from Media*, NPR (July 12, 2013, 4:59 PM), http://www.npr.org/blogs/thetwo-way/2013/07/12/201566829/justice-tightens-guidelines-for-obtaining-records-from-media, *archived at* http://perma.cc/5CZF-J9KS.

[190] *See* 28 C.F.R. § 50.10(g)(3) (2013)（司法省ガイドライン）（「複数のニュースメディアの電話料金記録が…通知なく差し押さえられる場合、令状に基づき情報が返還されてから45日以内に通知がなされなければならないものとする。但し、権限を有する司法長官補が45日を超えない範囲で通知の遅延を認めることができる。」）.

[191] *See* Philip Bump, *The Justice Department Secretly Seized AP Phone Records — on a Terror Leak?*, THE WIRE (May 13, 2013, 5:00 PM), http://www.theatlanticwire.com/politics/2013/05/justice-department-ap-phone-records/65184/, *archived at* http://perma.cc/AWT-92K3.

[192] *See* sources cited *supra* note 18.

[193] MERRILL JENSEN, THE NEW NATION: A HISTORY OF THE UNITED STATES DURING THE CONFEDERATION, 1781–89, at 430 (1950)（「ほとんどの新聞社は、1つの問題のあらゆる側面に関する内容を報じることがその公的な義務の一部をなしていると確信していた。たとえそれがある新聞社の見解と正反対のものであっても。」）; David A. Anderson, *The Origins of the Press Clause*, 30 UCLA L. REV. 455, 466 (1983)（多くの植民地の新聞は、党派的な内容の印刷に加えて、「公共の議論の場としても機能した」と指摘する）.

ある。[194]

修正第1条の文言に忠実な法のみを調べれば、事前抑制は異常なことで、法的には望ましいことではなく、可能な限り短い時間に限定されなければならないことが分かる。[195] 対照的に、国家的な監視国では、インフラストラクチャーを所有する会社に対する事前抑制は、広範に広がり、法的に優遇措置を受け、また永久に継続する可能性がある。*Pentagon Papers* 事件において政府が求めた事前抑制は異常なものに見え、国民的な注目を集めた。国家的監視国の事前抑制の特徴は、完全に当たり前のものとなり、ほとんど注目を集めないことである。それは、ありとあらゆる所に存在するため、全く目立たなくなる。

Ⅳ．結論：最新型の言論規制の目的

Ａ．従来型の規制の目的：萎縮効果と事後処罰

従来型の言論規制の目的と内容は、前デジタル時代における強制の可能性や前デジタル時代の技術を用いることによって形作られてきた。従来型の規制は、団体、場所、大量頒布のための前デジタル的な技術をコントロールしようとする。表現を広める行為がデジタルネットワークに移行する以前は、国家が禁止行為を事前に阻止することは比較的難しかった。それゆえ、ほとんどの従来型の言論規制は事後的なもの―犯罪訴追、課徴金、本などの対象物の押収又は廃棄―である。例えば、*New York Times Co. v. Sullivan* 事件は名誉毀損法に関するものであり、事後規制である。

従来型のモデルでは、事前の表現行為を抑止することは必ずしも不可能

---

[194] Lee, *supra* note 18.

[195] *See* Neb. Press Ass'n v. Stuart, 427 U.S. 539, 562 (1976)（「出版に対する事前抑制は我々の判例法において認知されている最も特別な救済手段である。」）; *Pentagon Papers*, 403 U.S. 713, 714 (1971)（全員一致）（「表現の自由に対する事前抑制のシステムは、当裁判所に違憲性の強い推定をもたらす。」（Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963) を引用）（引用表記は省略））; Freedman v. Maryland, 380 U.S. 51, 59 (1965)（「裁判所による最終的な実体判断が行われる前に課されるいかなる抑制も、同様に、妥当な司法判断と矛盾しない最も短い期間にその現状の維持が制限されなければならない。」）.

ではないが、その機会は、最新型の言論規制における場合よりも、より制限される。おおざっぱに言えば、前デジタル時代にも効果的な事前抑制が可能な状況は存在する。まず、国家は、出版・放送技術に許諾条件を課し、又は政府の資産に対するアクセスを制限することが可能でありかつ効果的である場合には、望ましくないと思われる活動が生じる前にそれを阻止することができる。第二に、国家は、言論が発せられる時を知ることができ、かつそれに対する司法上の差止命令による差止めが間に合う場合、望ましくない言論を阻止することができる。*Pentagon Papers* 判決は上記のうち2つ目の状況に関するものであった。

これら2つの状況を除き、通常、国家は言論が起こる前にそれを阻止してはならない。それゆえ、従来型の言論規制は、しばしば抑止に頼る。国家は人々に対して行動した結果を恐れる理由を与えることで望ましくない表現を阻止したいと望む。このために、国家は、妨害したいと思う表現行為をさせないようにする目的で、過度に広範で曖昧な規制を成立させることができる。国家は、保護されるべき活動を捕捉することは望まないかもしれないが、保護されるべきではない行動の全てが確実に抑止されることを望む。規制の観点（市民の自由の保護の観点ではなく）からは、ある行為が違法かどうかが不明確であることでさえ、悪いことではなく良いこととなり得る。

現代の修正第1条の法理が萎縮効果に焦点を当てることは、従来型の表現規制が達成しようとしたことと単純に表裏一体の関係にある。従来型の表現規制は国家がコントロールしたいと望む言論に対して萎縮効果をもたらすことを「欲する」。また、望ましくない言論に対する報復ないし処罰といった国家による脅威が公衆からはっきりと見え、広く認識されれば、それは大変有益なことである。同様に、表現活動の監視が公にされ、又は、監視される可能性が一般大衆に非常に分かりやすいものであれば、それもまた有益である。一般大衆がデモにおいて警察に氏名を知られたり、違法な言論によって人が逮捕されるのを見たりすることがないとしても、そういうことが現実にあるということを市民が知っていれば十分である。従来型の言論規制の要点は、行動しないよう説得・抑止することであり、すなわち、恐怖・不安・悲観・従順を生じさせることであると言える。

B．最新型の規制の目的：広範さ・分かりにくさ・事前抑止
― 萎縮効果から平穏な状態に置くこと（Chilling Out）へ

デジタルの世界では、異なる所に国家の行為や技術の力点が置かれる。新たな言論規制は、事前抑止に更なる可能性、すなわち伝統的な規制よりも更に効果的な可能性を提供する。表現の自由のインフラストラクチャーが規制や監視のための技術と融合しているため、国家は、望ましくない言論が発せられているとき、それをより発見しやすくなる。また、自ら直接、又は私人を監視と付随的な検閲に従事するよう誘うことによって、言論をブロックすることがより容易になるであろう。国家は、私人が望ましくない言論を探し、遅れさせ、選び出し、また完全にブロックするインセンティブを与えることができる。

確かに、伝統的な言論規制もなくなってはいない。最新型の言論規制においても、政府は財産権と監視能力を守るために各活動を萎縮させることができる。著作権法に基づいて認められる請求とそれに対するフェアユース抗弁の境界はしばしばはっきりせず、その結果、保護される表現がこれらの組み合わせにより萎縮する可能性がある。すでに指摘したとおり、NSLに付随する報道禁止命令は、企業が公開を試みることのないよう、「脅威を感じる」効果を生むように設計されている。

それにもかかわらず、デジタルネットワークが監視と予防をより容易にしたため、最新型の言論規制はブロッキングやフィルタリングといった事前の戦略をより多用する。こうして、大まかに言えば、従来型の言論規制は抑止と萎縮効果を際立たせ、最新型の言論規制は予防と分かりにくさ（又は不可視性）を際立たせる。

有害なコンテンツの監視とブロックがますます効果的になり、かつ広がりを見せるにつれ、萎縮効果を生じる従来型の言論規制アプローチはますます複雑になっている。疑わしい者だけが（又は主にそのような者が）監視の対象とされる世界から、政府と民間企業が分析、予防そして対抗措置を促進するためにできるだけ多くの人の情報を集める世界へと移行するにつれて、政府の統治戦略も変化する。

国家と民間のインフラストラクチャー所有者は、監視が一般公衆には気付かれないことを好むだろう。データ収集と分析の範囲と程度は、人々に自身は安全だが、絶えず観察されているわけでもないと感じさせるために

秘密とされるか、少なくとも分かりにくいものであるべきである。監視が人々にとって分かりにくいとき、人々は、政府や民間のインフラストラクチャー所有者が収集し、分析できる情報をより進んで明らかにするだろう。全く罪のない人について集められた情報は、国家が疑いを持つ者の行動を特定し、理解し、ブロックするのに役立つ。公衆が広がった監視活動に気付いている限り、政府も民間企業も、公衆がそれを服従や従順を引き出すために設計された恐ろしいものであることを理解しないで欲しいと思うだろう。逆に、政府と民間企業は、データ収集作業を、ごく自然で、厄介なものではなく、また無害なものであるように見せることを望むであろう。国家的監視国では、かつては「疑わしい」者だけの特権だった監視の経験は民主化し、普遍化し、また陳腐化する。監視の広がった世界では、国家と民間インフラストラクチャーの所有者は、ほとんどの人々に関し、萎縮効果を与えたいとは思っていない。その代わり、ほとんどの人々を平穏な状況に置きたい（chill out）のである。

要するに、最新型の言論規制の目的は常態化と不可視化（又は少なくとも分かりにくさ）である。そのために、単に処罰するのではなく、予防するための措置を採用し、またそれは自動的にかつ遠隔的に起こるようになっている。デジタル時代における言論の民主化の皮肉は、まさに、それがコントロールと監視の実践へと繋がっていることである。他の有名な言葉で言い換えてみると、インターネット上では、誰もあなたが犬だとは気付かない―政府と民間インフラストラクチャーの所有者を除いて。

New York Times Co. v. Sullivan 判決と *Pentagon Papers* 判決は、言論規制に使われた20世紀の技術に対する20世紀の対応である。しかし、言論を規制する技術はまだ固まっていない。言論を促進する技術も同様である。ポストニューディール時代の表現の自由の擁護者は、従来型の規制技術に対応する憲法上の保障を作り上げる方法を生み出さねばならなかったが、それとまさに同様に、最新型の言論規制の世界で表現の自由の原則を再創造することが、現在の世代に課せられている。表現の自由の信条は普遍的なものかもしれないが、言論規制の手段は変幻自在に変わり続けている。それに対する我々の対応も同じようにあるべきである。

［訳者付記］

本稿は、Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296 (2014)の翻訳である。

光栄なことに訳者１名（樫尾）は、所用で渡米した際にYale Law Schoolを訪れ、原著者のJack M. Balkin教授と面談する機会を得た。同教授は聡明で、かつ本稿の各所に表れているような現代的な感覚を感じさせる方であった。

ところで、本稿の原題のタイトルには、“new school/old school”という日本語訳が難しい言葉が使われており、上記面談の際、この言葉を選んだ意図について尋ねた。Balkin教授によると、これは、Hip Hopの世界で1980年代中頃を境にold school / new schoolと呼ばれる楽曲のテイストの変化があることと、本稿で指摘されている言論規制のテクニックの変化とを掛けた、一種のジョークであるとのことであった。このジョークの翻訳を巡り、訳者らは長い議論を行い、「新派の/旧派の」、「今風な/古風な」、「新手の/古典的な」などの数々の案が出た。最終的に学術論文としての性格、対比や語感を重視して「従来型と最新型」に落ち着くこととなったが、原題のニュアンスが失われた感は否めないため、ここでBalkin教授の意図をご紹介することで代えさせて頂きたい。

最後に、本稿の翻訳をご了承頂いたBalkin教授、また翻訳発表の場を頂いた田村善之教授及び校正作業でお世話になった髙橋直子特任助手（北海道大学大学院法学研究科）に改めて御礼申し上げる。