判例研究：暗号化されたハードディスクの内容の復号（暗号解除）を大陪審が罰則付召喚状により命ずることは連邦憲法修正第 5 条に違反するとされた事例―United States v. Doe, 670 F.3d 1335 (11th Cir. 2012)―

湯淺　墾道[1]

概 要

第 11 巡回区連邦控訴裁判所は、令状により押収したコンピューター、外付けハードディスクドライブ等のハードディスクが、暗号化ソフトウェアにより暗号化されており、ハードディスクに保存されているファイルにアクセスできない場合、大陪審が発出する罰則付召喚状によって、暗号化されたハードディスクの復号化（暗号の解除）を行いハードディスクの内容を証拠として提出するように命じることは、被告人が復号化して提出した内容が被告人に不利な証拠として利用されて被告人の自己負罪を招く可能性があるので、アメリカ合衆国憲法修正第 5 条が規定する自己負罪拒否特権に違反すると判断した。このため被告人は復号化を強制されないとし、大陪審の召喚状の命令に従わず暗号化されたハードディスクの復号化（暗号の解除）とハードディスクの内容の証拠提出を拒否したという理由で被告人に民事的裁判所侮辱を科した連邦地方裁判所の判断は、誤りであるとして差し戻した。

1　事案の概要

2010 年 10 月、警察は児童ポルノ所持の疑いで内偵中だった事案について、容疑者のものと思われる Youtube のアカウントにアクセスしている IP アドレスをもとに捜査を行った結果、当該アカウントの所持者である容疑者がカリフォルニア州内のホテルからアクセスしていることを突き止めた。このため容疑者が滞在していると思われるカリフォルニア州内のホテルの部屋を捜索するための令状の発給を裁判所に申請し、捜査員がデジタル・メディアと、当該デジタル・メディアにアクセスするために必要となる暗号化機器又はコードを押収する許可を得た。令状に基づき、捜査員はホテルの部屋を捜索して、本件被告人を逮捕し、被告人が所有する 2 台のラップトップ・コンピューターと、5 台の外付けハードディスクを押収した。連邦捜査局（FBI）のデジタル・フォレンジック専門家がこれらの解析を試みたものの、暗号化ソフトウェアによりハードディスクが暗号化されていたため、ハードディスク

1 情報セキュリティ研究科 教授

の内部領域にはアクセスすることができなかった。

その後、被告人を起訴するかどうかについて決定するため、大陪審による審理が行われることになった。

大陪審は 2011 年 3 月 25 日に罰則付召喚状（subpoena)を発出し、被告人に対して、押収されたデジタル・メディアのすべてのフォルダーのいかなる内容についても、暗号化されていないコンテンツを証拠提出(product)するように求めた。暗号化ソフトウェアによりハードディスクが暗号化されており、ハードディスク内に児童ポルノが保存されているのかを確認できないためである。しかし被告人は、当該令状に従うことは、何人も刑事事件において自己に不利な証人になることを強制されないとする連邦憲法修正 5 条の自己負罪拒否特権の保障に違反すると主張した。

このため 2011 年 4 月 19 日、連邦検事と被告人はフロリダ州北部地区連邦地方裁判所の審理に出廷し[2]、連邦検事は裁判所に対して、被告人の自己負罪拒否特権を、被告人がハードディスクの暗号化されていない内容を証拠提出する行為には、適用しないように要請した。裁判所は、連邦政府がハードディスクの復号化された内容を証拠として使用することについては、被告人に自己負罪拒否特権を与えないとする命令を発出した。

これに対して被告人は、命令に従ってハードディスクを復号して暗号化されていない内容を証拠提出することを、拒否した。

このため検事は、命令に従うことの拒否は民事的裁判所侮辱にあたるとし、被告人に対して命令を拒否する根拠を示すように命ずることを裁判所に求めた。裁判所はこれに応じ、命令に従わない根拠を示すことを被告人に命じた。被告人は、政府がハードディスクの復号化された内容を証拠として使用することは、何人も刑事事件において自己に不利な証人になることを強制されないとする連邦憲法修正 5 条の自己負罪拒否特権の保障に違反すると主張した。しかし裁判所は被告人の主張を認めず、民事的裁判所侮辱により被告人を拘禁することを命じたので、被告人が不服として第 11 巡回区連邦控訴裁判所に訴えたものである。

2　判旨

トジョフラット(Tjoflat)判事が執筆した判決の大要は、次のとおりである。

I

本件の発端は、児童ポルノの捜査の過程で 7 台のデジタル・メディアの捜査を合法的に行ったことである。

2010 年 10 月、警察は児童ポルノ所持の疑いで内偵中だった被告人がカリフォルニア州のホテルに滞在していることを突き止めた。警察は裁判所に被告人が滞在しているホテルの部屋を捜索するための令状の発給を申請し、捜査員がデジタル・メディアと、当該デジタル・メディアにアクセスするために必要となる暗号化機器又はコードを押収する許可を得た。令状に基づき、捜査員は 2 台の Dell 社製のラップトップ・コンピューターと、5 台の

2 その際、被告人は弁護士の付き添いなしで出廷した。United States v. Doe (In re Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1338 (11th Cir. Fla. 2012).

外付けハードディスクを押収した。連邦捜査局（FBI）のデジタル・フォレンジック専門家がこれらの解析を試みたものの、ハードディスクの一部領域にはアクセスすることができなかった。

大陪審は 2011 年 3 月 25 日に罰則付召喚状（subpoena)を発出し、被告人に対して、「デジタル・メディア内のすべてのフォルダーのいかなる内容」についても、「暗号化されていないコンテンツ」を証拠提出するように求めた。しかし被告人は、当該令状に従うことは、何人も刑事事件において自己に不利な証人になることを強制されないとする連邦憲法修正 5 条の自己負罪拒否特権の保障に違反すると主張した。

押収されたハードディスク等が被告人のものであることについては、争いはない。したがって、陪審よりも前の大陪審の段階で、政府が被告人から押収したハードディスクの内容を復号化して内容に児童ポルノが含まれていることを明らかにし、児童ポルノ所持を禁ずる連邦法違反として起訴できるかどうかを決定することは、修正第 5 条により禁じられるかどうかという点が問題となる。被告人は、政府が被告人から押収したハードディスクの内容を復号化して内容に児童ポルノが含まれていることを明らかにするのは、大陪審における被告人の証言を派生的(derivative)に利用することになると主張した[3]。

FBI のデジタル・フォレンジックの専門家は、押収したデジタル・メディア類に保存されていたデータ類は 5 テラバイト以上であると証言した。ハードディスクは「TrueCrypt」というソフトウェア[4]によって暗号化されており、データを解析のためにハードディスクから抽出することができず、ファイル類を発見することもできなかったという。しかし専門家は、暗号化されたハードディスクの中には、データが保存されている可能性が高いと証言した。この証言を裏付けるため、政府側は非規則的な文字列と数字の配列を提示したが、政府側はこれは暗号化されたデータの一部であると主張した。他方、被告人側からの反対尋問の際、証人はハードディスクが暗号化されていたとしても内部に全くデータが保存されていないということはあり得るとも証言した。

なおデジタル・フォレンジックによって、2 種類のパスワードを認識することができたが、どちらのパスワードを入力してみても、特に情報は得られなかった。

II

以下に被告人の主張を検討してみる。

地方裁判所は、被告人に暗号化されていないコンテンツを証拠提出することを命じ、それを拒否したとして民事的裁判所侮辱により被告人に制裁を科した。これによって、復号化されていないコンテンツを被告人の起訴のために政府が利用したとしても、それは修正 5 条の自己負罪拒否特権によって保護されている強制的な証言の派生的利用には当たらない、と地方裁判所は結論づけたことになる。おそらく、地方裁判所は被告人に復号化させてハードディスクドライブのコンテンツを証拠提出させることは、「証言」には当たらないと考えたのであろう。

3 派生的手段によって得られた証拠は、違法な捜索押収によって得られたものとして、証拠能力がないと解される。

4 TrueCrypt License の下で無償で利用できる暗号ソフトウェアで、暗号化された仮想ディスクを作成・利用することができ、Windows 版 TrueCrypt ではシステムドライブ自体も暗号化することができるようになっていた。Windows XP のサポート終了に合わせて、TrueCrypt の開発も 2014 年 5 月で終了している。このため、現在は BitLocker に移行することが勧奨されている。http://truecrypt.sourceforge.net/

しかし、復号化させてハードディスクドライブのコンテンツを証拠提出させることは、修正第 5 条の保護の問題を惹起するものである。これは証言に該当しうるものであるし、修正第 5 条の保護は、政府によるハードディスクドライブの利用に対しても適用される。

ゆえに地方裁判所は 2 つの誤りを犯している。1 つは、被告人による復号化とコンテンツ証拠提出は「証言」にはあたらないとしたことである。もう 1 つは、被告人に特権を付与する際の誤りであり、政府が被告人に復号化とコンテンツ証拠提出をさせることへの特権は制限しておきながら、復号化とコンテンツ証拠提出によって開示された証拠の派生的利用は許容したことである。

A.

ここで問題になっているのは、政府は修正第 5 条の文脈でいうところの「証言」を求めたのかどうかという点である。被告人による復号化とコンテンツを証拠として提出する行為が「証言」にあたるかどうかについては、合衆国対ハッベル判決[5]、フィッシャー対合衆国判決[6]という 2 つの連邦最高裁の判決が存在する。政府は証言にあたることは否定しており、被告人に対して求めたのは、すでに存在するファイル類と任意に作成されたファイル類を手交することだけであると主張する。ハードディスクの隠された領域の中にあるファイル類だけに限るのであれば、それは証言にはあたらない。

しかし、ハードディスクの中の内容が証言に当たるかどうかは、ここでは問題とはならない。ここでの問題は、証拠を提出するという行為が、明示的または黙示的に重要な事実を証明するものとなる場合には、当該証拠提出行為は修正第 5 条の保護を受けるに値しうる、ということである[7]。ゆえに、被告人の復号化と証拠提出という行為が証言に当たるかどうかの検討を行う。

1.

フィッシャー対合衆国判決は、第 3 巡回区連邦控訴裁判所と第 5 巡回区連邦控訴裁判所における 2 件の内国歳入庁の調査に関する判決を、連邦最高裁が裁量上訴(certiorari)により審理したものである。

それぞれの事案で、内国歳入庁は納税者の代理人となっている弁護士に対して、納税者の領収書その他の書類の提出を召喚状(summon)により求めた。しかし弁護士は、文書類は依頼人と弁護人との間の秘密によって保護されており、弁護士自身の修正第 5 条の自己負罪拒否特権によっても守られているとして、提出を拒否した。このため連邦地方裁判所は弁護士たちに対して召喚状を守るように求める命令を発出し、弁護士側はこれを不服として連邦控訴裁判所に訴えたものである。

連邦最高裁は、弁護士が書類を提出する行為は、弁護士自身の修正第 5 条の自己負罪拒否特権の保護の対象にはならないとした。また納税者自身については、召喚状に従って文書を証拠提出することは、証言にはあたらないとした。政府は、文書類が存在し納税者がそれを占有していることを知っており、納税者の知性(mind)を使用することなく他

5 United States v. Hubbell, 530 U.S. 27 (2000).
6 Fisher v. United States, 425 U.S. 391 (1976).
7 Fisher v. United States, 425 U.S. 391, 410 (1976).

の手段によって原本性を証明することができるからである。目的となっている証拠の所在、存在および原本性が合理的な特定性の下に明らかになっている場合には、個人の知性が使用されることはないから、修正第 5 条の保護は適用されない。

フィッシャー対合衆国判決の 24 年後、最高裁は、合衆国対ハッベル事件の判決を下した。

本件では、大陪審は被告人に罰則付召喚状を発出して、ホワイトウォーター開発会社に関係する書類を提出するように命じた。被告人はこれに従い、13120 頁にも及ぶ文書類を提出した。大陪審は提出された文書類を調査し、それに基づいて被告人を複数の連邦犯罪で 10 の罪状により起訴することを決定した。これに対して被告人は、起訴は被告人の特権によって保護されている文書類だけに基づいて行われているとして、連邦地方裁判所に起訴の取消を求めて訴えた。連邦地裁はこれを認めたため、政府は連邦最高裁に訴えたというものである。

連邦最高裁は裁量上訴により訴えを受理し、被告人の証拠提出行為は、証言にあたるものであり、修正第 5 条の適用を受けると判断した。フィッシャー判決との相違について、最高裁は、「フィッシャー事案では、政府は文書類を弁護士が保持しており、それが存在しており原本であることを作成者からは独立して証明することが可能であった。本件では、最終的に被告人の作成に係る 13120 頁にも及ぶ文書類が存在していることやその内容について事前に知識を有していたことを、政府は何ら示していない」と判示した。

2 件の最高裁判決からは、次のような原則を描き出すことができる。ある証拠提出行為は、ある証拠物が存在していて、それが召喚状を発出された個人の占有もしくは管理下にあるとき、または原本であるときに、当該行為が事実を明示的または黙示的に証明するものである場合には、証言となりうる。当該証拠提出行為が証言にあたるかについては、事実の明示的または黙示的に示すため、個人に「自身の知能の内容」を使用することを政府が強制するかどうかが一つの基準となる[8]。

ただし、最高裁は証拠提出行為が証言にはあたらない場合も示している。

政府が物理的な行為を単に強制する場合には、修正第 5 条の保護は適用されない。たとえば、個人がその知能の内容を使用することは命じられていないような場合である。最も有名な例は、文書類が保管されている金庫の鍵自体の提出の強制であろう[9]。また、「自明の理(foregone conclusion)」法理の下では、証拠提出行為は証言にはあたらない。召喚状の対象となっている証拠物の存在、所在、占有または原本性を政府が「合理的な特定性」をもって示した場合には、証拠提出を命じたとしてもそれは既知のものであるので、証言にあたるかもしれない要素を「自明の理」とする[10]。このため、この場合は、証拠提出行為は証言にはあたらなくなるのである。

2.

以上に論じた枠組みを用いて、本件の事実関係を検討する。

本件において、ハードディスクを復号化して内容を証拠提出するという行為には、修正第 5 条の保護が及ぶ。その理由は、(1)被告人がハードディスクを復号化して内容を証拠

8 Curcio v. United States, 354 U.S. 118, 128 (1957).
9 Doe v. United States, 487 U.S. 201 (1988).
10 Fisher v. United States, 425 U.S. 391, 411 (1976).

提出するという行為は証言にあたり、単なる肉体的な行為ではないこと、(2)復号化と証拠提出に関連する明示的・黙示的な事実のコミュニケーションは、「自明の理」とはいえないこと、である。

もし被告人が地方裁判所の命令に従っていれば、被告人はその知性の内容を、自らを有罪にするため、または政府に自らを有罪にする証拠を得させるために、使用することになっていたであろう。さらに、政府は暗号化されたハードディスクの中にファイルが存在し、被告人がそれにアクセスしたか、被告人自身がそれを暗号化したということについて、合理的特定性をもって示していないから、ここでは「自明の理」法理は適用されない。

修正第 5 条は、被告人がハードディスクを復号化して内容を証拠提出するという行為を拒否したことを保護する。というのは、復号化して内容を証拠提出するという行為は証言にあたり、政府は「自明の理」法理が適用されるということを挙証していないからである。

B.

被告人が与えられる特権について検討する際、どのような行為が実際に特権の対象となるのかという点と、政府が将来の起訴において利用すると派生的利用とされるのはどのようなものか、という点に着目しなければならない。

最高裁の先例は、証拠として利用することから保護する特権と、派生的利用の禁止は、修正第 5 条の自己負罪拒否の射程の下で両立すると示している。証拠として利用することから保護する特権には例外も認められるが、政府はそれを示していない。ハードディスクを復号化して内容を証拠提出するという被告人の行為は証言にあたるから、それを命じる際には、修正第 5 条の保護と両立する特権が要求される。その特権は、被告人を有罪とするために利用すること及び派生的利用することから、被告人を保護するものである。

政府は、被告人が復号化して内容を証拠提出してハードディスクは本件に限って利用し、将来の起訴に利用することはないと被告人に書簡を送っている。しかし政府は、自己負罪拒否特権を有する証言として復号化して提出された内容を、証拠として利用することが可能であり、そのような利用は修正第 5 条の保護に反する。ゆえに、被告人が復号化して内容を証拠提出することにより、被告人の自己負罪を招く可能性がある以上、被告人は復号化を強制されない。

III

当法廷は、被告人は修正第 5 条の自己負罪拒否特権について適切に主張を行ったと判断する。これに対して、政府は被告人に修正第 5 条の自己負罪拒否特権を付与しないことを選択し、地方裁判所はそれに黙従した。被告人は、ハードディスクのコンテンツを暗号化せずに証拠提出することを拒否したが、この拒否は正当化されるものであり、地方裁判所が被告人に民事的裁判所侮辱の制裁を科したのは誤りである。ゆえに地方裁判所の判決は差し戻す。

3　若干の考察

3.1　暗号化と刑事捜査

暗号化が情報セキュリティ・サイバーセキュリティの確保における有力な手段であることは、広く認識されている。また、暗号化が政府によるプライバシー侵害に対抗する強力な武器であることも、かなり以前から認識されている。特にアメリカにおいては、総合犯罪防止安全市街地法(Omnibus Crime Control and Safe Streets Act of 1968)[11]、外国情報活動監視法(Foreign Intelligence Surveillance Act of 1978)[12]、通信傍受法(Communications Assistance for Law Enforcement Act of 1994)[13]、愛国者法(Patriot Act of 2001)[14]等の規定によって広く通信傍受が認められており、特に外国情報活動監視裁判所(United States Foreign Intelligence Surveillance Court)は、2004 年から 2012 年までの間に 15100 件の令状を発給し、令状発給を退けたのはわずか 7 件であったと報じられているというような状況であることから[15]、このような広範な通信傍受の動きに対抗するための有効な手段として、暗号化はユーザー及び端末製造販売者の両方で活用されてきた。

他方で、最新のデジタル・フォレンジック技術[16]によっても解析できないような強力な暗号化を、廉価な機器や無料・安価なソフトウェアによって簡単に行うことができるようになった結果、暗号化によって合法的な犯罪捜査が困難となり、結果的に犯罪者を利するものとなっていることも事実である。

捜査当局側からみると、暗号化が捜査の支障となっている状況は顕著となってきており、連邦司法省のレジー・カードウェル(Leslie Caldwell)次官補は、2015 年 1 月に「暗号化の意義とセキュリティの重要性は理解しているが、それが『無法地帯(zone of lawlessness)』を生み出さないことを願わずにいられない」と述べている[17]。もっとも、このこと自体は今に始まった話ではなく[18]、アメリカ政府は暗号を解読したり、暗号化の強度を弱めたりすることを以前から試みている。その手法には、暗号の自力解読、強力な暗号の使用制限、暗号化された制御をかいくぐることができる「裏口」の実装の義務づけ、何らかの方法による暗号鍵の入手という 4 つがあるという[19]。また司法省、国立司法省研究所(National Institute of Justice)、シンクタンクのランド社(Rand Corporation)、デンバー大学等からなる共同プロジェクトのリポートは、デジタル証拠に関連する課題と解消策の一覧を示しているが[20]、その中でも携帯電話の暗号化とパスワードの問題が指摘されている。

---

11 18 U.S.C. § 2518.
12 50 U.S.C. ch. 3.
13 47 U.S.C. § 1001 et. seq.
14 115 STAT. 272 (2001).
15 Evan Perez, *Secret Court's Oversight Gets Scrutiny*, WALL STREET JOURNAL, June 9, 2013, http://www.wsj.com/articles/SB10001424127887324904004578535670310514616.
16 デジタル・フォレンジック技術に関係する近時の法的課題については、前田恭幸「刑事訴訟におけるデジタル・フォレンジックツールの課題（上）」捜査研究 789 号（2016 年）12 頁以下などを参照。
17 Jason Koebler, *Tor and Encryption Have Created a 'Zone of Lawlessness,' Justice Department Says,* VICE (Jan. 27, 2015, 1:35 PM), http://motherboard.vice.com/read/torand-encryption-have-created-a-zone-of-lawlessness-justice-department-says.
18 Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171 (1996).
19 指宿　信「Apple 対 FBI 問題を考える」法学セミナー2016 年 7 月号（2016 年）6 頁。
20 Goodison, Sean E., Robert C. Davis and Brian A. Jackson, Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence 23 (2015). http://www.rand.org/pubs/research_reports/RR890.html.

今日、パソコンだけではなく、タブレットやスマートフォンその他の端末には、何らかのロック機能やパスワードによる保護機能が装備されているのが普通である。さらに、自動車や家電製品など、多くの製品の中にコンピューターが内蔵されるようになっており、これらの中にもパスワードやパスコード無しには内部のデータにアクセスできないものがある。このためレポートでは、端末自体の暗号化に対しては「暗号に対処する代替手段を開発する」としているが、現実には、高度な暗号技術に対抗してそれを復号する技術を開発することは困難であるとされる。

なお本稿でいう「暗号化」は、特定の技術を用いてデータを暗号化(encrypted)、秘密化(enciphered)、符号化(encoded)、モジュール化(modulated)もしくは不明瞭化(obfuscate)することにとどまらず、暗証番号（パスコード）やタッチコード等を用いて端末をロックし、それらを用いてロックを解除しないと内部のデータ等にアクセスできないようにすることも含めた広義のものを指すものとしたい。

3.2 復号化（暗号解除）の方法と修正第 5 条

押収したコンピューターや携帯電話等のデータが暗号化されている場合、捜査機関側はデジタル・フォレンジック等の技術によってそれを解析しようとする。しかし、捜査機関側でも復号化または暗号解除ができない場合、捜査機関側にはどのような手段が残されているであろうか。

考えられる第 1 の手段は、暗号化を施した被疑者等に対して暗号を解除する方法や、パスコード・パスワード等の開示を強制し、開示させたものを使って、捜査機関等が暗号を解除することである。

第 2 の手段は、暗号を解除する方法（パスコード）等の開示を強制することはしないが、本件で問題となったように、暗号化を施した被疑者に対して復号化（暗号の解除）を法的に強制することである。その中には、本件で問題となっているような復号化（暗号解除）したものの提出を命じるという方法も含まれよう。この場合は、暗号を解除する方法や、パスコード・パスワード等自体は、捜査機関等は取得しないことになる。

以下に、それぞれの方法と修正第 5 条との関係について検討してみるが、結論から先に述べると、第 1、第 2 の手段ともに連邦最高裁の判断は、被疑者等に対して暗号化された端末等の復号、暗号化の解除を強制的に命じることの合憲性について、それが人の知能の内容が関係するか、それとも単に身体を物理的に動作させるにすぎないかによって異なると解されている。つまり、連邦最高裁は、強制する内容に被疑者の知性が伴うか、それとも単なる肉体的行動であるかによって判断しており、「知性・肉体基準」とでも評すべき基準を用いているのである。

さらに、全令状法(All Writs Act)[21]を活用して、事案とは直接の関係がないが復号・暗号解除の能力を有する第三者に対して復号・暗号解除の支援を法的に要請して、その支援を得て捜査機関等が暗号を解除するという手段もある。これが近年いわゆる iPhone ロック解除問題で是非が問われている方法である[22]。

21 28 U.S.C. § 1651.
22 湯淺墾道「全令状法と iPhone 問題に関する若干の考察」電子情報通信学会技術研究報告 116 巻 71 号（2016 年）43 頁以下を参照。

3.2.1　復号のための記号やパスワードの開示強制と修正第 5 条

コンピューターや携帯電話等のデータが暗号化されていたり、端末自体がロックされたりしていて解析ができない場合、復号のための記号やパスワードを被疑者に強制的に陳述・開示させるというようなやり方は、修正第 5 条に違反するのであろうか。

連邦最高裁は、コンピューターや携帯電話等にパスワードを強制的に入力させることの合憲性について、判断を示していない。しかし、通常は数字やアルファベットの組み合わせで生成されるパスワードを強制的に明らかにさせることは、憲法上の問題が生じる可能性があるとされる。

連邦最高裁は、単なる肉体的な行為を強制して証拠を提出させる場合については、一定の条件の下に許容してきた。これに対して、復号や暗号化の解除には単なる肉体的ではなく、人の知能が関係する。その際、個人にその知能の内容を強制的に表現させることは修正第 5 条により禁じられているというのが、1957 年に連邦最高裁が下したクルシオ対合衆国判決[23]以来の一般的な理解である[24]。

端末等を暗号化する暗号の多くは、ID や PIN、パスワード等のように、数字や文字、記号の組み合わせにより構成される。この組み合わせを人が生成した場合には、それは人の知能の営為の結果であるということになる。また、人がパスワード等を生成したのではなく機械的に生成したものであったとしても、それを人が記憶していた場合にこれを明らかにさせることは、記憶していた暗号を想起するという知能の営為がやはり働く。このような場合にそれを強制的に明らかにさせることは、禁じられていると解されてきた。

これに対して、単なる肉体的な行為を強制して証拠を提出させる場合の典型例として挙げられるのが、本件判例でも引用されている証拠物を保管している金庫の鍵の提出を命じたという事例である[25]。鍵を物理的に提出させることには、知能の内容を強制的に表現させるという要素はなく、身体を物理的に動作させるにすぎないと連邦最高裁は判示している。

この二つの場面の両方が関係するのが、「左に何回、右に何回、それから左に何回」とダイヤルを回し鍵の組み合わせをして解錠するような仕組みの金庫のダイヤル式の鍵を開けさせるという場合である。

この場合について、連邦最高裁は、1988 年のドー対合衆国判決において、刑事事件の証拠物が入っている金庫の鍵の引き渡しを命じることはできるが、壁金庫(wall safe)のダイヤル鍵の解錠のために強制的に鍵の組み合わせを命じることはできないと判示している[26]。

刑事事件の証拠物が入っている金庫の鍵の引き渡しを命じることはできるというのは、それが単なる肉体的な動作だからである。しかし、ダイヤル鍵の解錠のために強制的に鍵の組み合わせを命じることはできない。というのは、それが肉体的な行為にとどまらず、ある組み合わせを頭脳の中で考案するという内的な知的行為、すなわち知性(mind)に関する行為だからである。ゆえに、それを外的に表現することを強制することはできないというのである。

23 Curcio v. United States, 354 U.S. 118, 128 (1957).
24 Steve Posner, *Can a Defendant be Compelled to Provide an Encryption Key?*, 2012 EMERGING ISSUES 68, 38 (2012).
25 Doe v. United States, 487 U.S. 201 (1988).
26 Doe v. United States, 487 U.S. 201, 210 (1988).

3.2.2 復号化（暗号解除）の強制・復号化（暗号解除）した内容の提出の強制と修正第 5 条

次に、暗号化を施した被疑者に対して復号化（暗号の解除）を法的に強制することと修正第 5 条との関係について検討したい。

本件は、大陪審の罰則付召喚令状に従わなかったという理由で民事的裁判所侮辱(civil contempt)[27]の制裁を科されたことを不服として、被告人が連邦控訴裁判所に訴えたという事例であるが、ここでは、被疑者に復号化（暗号解除）を行わせて、内容の提出を強制することの可否が問われている。

本件では、児童ポルノ所持の疑いで警察は令状を得て被告人のラップトップ・コンピューター、外付けハードディスク等を押収した。FBI のデジタル・フォレンジックの専門家がデータの解析を試みたが、被告人が「TrueCrypt」というソフトウェアを利用してハードディスクを暗号化していたので、FBI のデジタル・フォレンジックの専門家も、押収したすべてのディスクに「TrueCrypt」を利用して暗号化されていた内容を復号してディスクの中に保存されていたファイル等を抽出することはできず、解析を行うことができなかった。

このため、被告人を起訴するかどうかを評決する大陪審の審理に付された際、大陪審は罰則付召喚令状によって、ディスク類のすべてのファイル等につき、被告人に暗号化されていないコンテンツを証拠提出することを求めた。暗号化されていないコンテンツを証拠提出することとは、暗号化されているものを復号化（暗号化を解除）し、誰でも見られるような状態にするということに他ならない。したがって被告人は暗号の復号（暗号化の解除）を行った上で、暗号化されていないコンテンツを証拠提出することを求められた、ということになる[28]。

これに対して被告人は、一貫して暗号の復号（暗号化の解除）を行った上で、暗号化されていないコンテンツを証拠提出することを拒否した。これは推測の域を出ないが、おそらく押収されたコンピューターや外付けハードディスクの中には、被告人によって児童ポルノ類が保存されていたのであろう。それらが提出されれば、被告人が有罪判決を受ける結果となることは容易に想像できる。そもそも、被告人が「TrueCrypt」というソフトウェアを利用してハードディスクを暗号化していたのも、万が一、司直の手が入った場合に備えてのことだったのかもしれない。

被告人の主張は、政府がハードディスクの復号化された内容を証拠として使用することは、何人も刑事事件において自己に不利な証人になることを強制されないとする連邦憲法修正 5 条の自己負罪拒否特権の保障に違反するというものである。

この主張について、本判決では、次のように被告人の主張を認めている。

本件では、被告人による復号化とコンテンツを証拠として提出する行為が「証言」にあたるかどうかについて、主として合衆国対ハッベル判決[29]、フィッシャー対合衆国判決[30]という 2 つの連邦最高裁の判決に依拠して判断している。

本件では、ある証拠物が存在していて、それが召喚状を発出された個人の占有もしくは管理下にあるとき、証拠を提出するという行為が事実を明示的または黙示的に証明するも

27 差止命令を無視したりして、故意に裁判所の命令に従わないことで、制裁として拘禁又は罰金が科される。
28 United States v. Doe (In re Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1338 (11th Cir. Fla. 2012).
29 United States v. Hubbell, 530 U.S. 27 (2000).
30 Fisher v. United States, 425 U.S. 391 (1976).

のである場合には、その証拠提出行為は証言となりうるとする。さらに、当該証拠提出行為が具体的に証言に該当するかの判断にあたっては、個人に「自身の知能の内容」を使用することを政府が強制するかどうかが一つの基準となるとしている[31]。つまり、提出にあたって単に身体を物理的に動作させるのではなく、個人の知能の内容を使用する必要がある場合は、提出行為自体が証言になりうるというのである。本件では、「復号化させてハードディスクを提供させることは、容疑者の知性(mind)の内容を使用するものであり、単なる肉体的な行為とはいえない」としている[32]。

ただし連邦最高裁は、証拠提出行為が証言にはあたらない場合も示している。それが「自明の理(foregone conclusion)」法理であり、召喚状の対象となっている証拠物の存在、所在、占有または原本性を政府が「合理的な特定性」をもって示した場合には、証拠提出を命じたとしてもそれは既知のものであるので、証言ではなく「自明の理」であるとする[33]。このため、この場合は、証拠提出行為は証言にはあたらないということになる。

3.2.3　全令状法の利用

押収したコンピューターや携帯電話等のデータが暗号化され、捜査機関側でも復号化または暗号解除ができない場合、アメリカにおいては全令状法(All Writs Act)[34]を活用して、事案とは直接の関係がないが復号・暗号解除の能力を有する第三者に対して復号・暗号解除の支援を法的に要請するという方法が残されている。

この法律は、もともとは 1789 年に制定された司法部法(Judicially Act)[35]という法律の一部であり、1911 年に現在の形になった。条文は、次の 2 条からなる。

> (a)連邦最高裁判所と連邦議会によって設立された全裁判所は、その権限を行使する上で必要もしくは適切であり、かつ法の慣習及び原理の上で許される全令状を発給することができる。
>
> (b)代替令状もしくは仮命令は、管轄権を有する最高裁判所裁判官もしくは（下級裁判所の）裁判官によって発給されることができる。

この法律によれば、連邦最高裁判所と連邦議会によって設立された全裁判所はその権限を行使するためにはどんな令状でも出すことができることになるが、連邦最高裁は 1948 年のプライス対ジョンストン判決において、全令状法は、「法の合理的な終結(the rational ends of law)」を達成するために連邦議会によって認められた手続的な手段であると解している[36]。この判決以降も、連邦最高裁はこの法律に基づく令状を出すことができる条件を、他の法律上の手段がない場合、連邦裁判所自身が管轄権を持っている場合、連邦裁判所の権限を行使する上で必要または適切である場合、令状の内容が議会によって制定された法律に反しない場合、に限定している[37]。

31 Curcio v. United States, 354 U.S. 118, 128 (1957).
32 United States v. Doe (In re Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. Fla. 2012).
33 Fisher v. United States, 425 U.S. 391, 411 (1976).
34 28 U.S.C. § 1651.
35 Judiciary Act of 1789, ch. 20, §§ 13-14, 1 Stat. 73, 81-82 (codified as amended at8 U.S.C. § 1651).
36 Price v. Johnston, 334 U.S. 266, 282 (1948).
37 Dimitri D. Portnoi, *Resorting to Extraordinary Writs: How the All Writs Act Rises to Fill the Gaps in The Rights of Enemy Combatants*, 83 N.Y.U.L. REV. 293, 299 (2008).

刑事事件の捜査との関係において、連邦裁判所は、全令状により法被疑者や被疑者と直接の関係がある者だけではなく、被疑者と直接関係のない者に対しても命令を下すことができるとしている。その先例は、1977 年の合衆国対ニューヨーク電話会社判決である[38]。

本件では、ニューヨーク市内で違法賭博を行っている可能性のある企業が捜査の対象となり、FBI は、当該企業が使用していた 2 台の電話機からダイヤルを回した先を記録する装置(pen register)を取り付け、情報を提供する支援をサウスウエスタン・ベル電話会社(Southwestern Bell Telephone Company)に要請した。しかし同社は拒否した。同社が支援を拒否したのは、政府がネットワークにアクセスした場合、政府による「無差別的プライバシー侵害」を帰結することになることを恐れたためであるとされる[39]。このため FBI は全令状法に基づき、電話会社に対して記録装置を取り付け情報提供すると共に FBI 捜査官を支援する命令を発出することをニューヨーク州南部地区連邦地裁に求めた。1976 年 3 月 19 日、連邦地裁は FBI の主張を認めて、電話会社に対し記録装置を取り付ける命令を発出した。これに対して電話会社側は、技術的支援を捜査機関に提供する命令について、1970 年に第 2 巡回区連邦控訴裁判所が下した先例[40]に基づいて、異議を申し立てた。

第 2 巡回区連邦控訴裁判所は、連邦裁判所が被疑者と直接関係のない第三者に対して命令を下すことはできないとして、電話会社の異議を認めた[41]。これに対して連邦最高裁は、連邦控訴裁の判断を覆した。ホワイト(White)判事執筆の法廷意見は、「私人である市民は、要請を受けたときには法執行機関に対して援助を提供する義務を有する」[42]と判示し、その論拠として後に連邦最高裁判事となるカードウゾ(Cardozo)判事がニューヨーク州最高裁判事時代に執筆した「エドワード 1 世の時代から、市民を国家の司法を執行するために招集することは許される」という判決文[43]を引用した。そして、「全令状法に基づいて連邦裁判所が第三者に対して無制限に命令を出すことができるというわけではなく、不合理な負担を課すことは許されない。しかし、本件における命令の内容は、全令状法によって明確に授権されたものであり、連邦議会の立法趣旨にも合致するものである」と判断したのである。

全令状法の問題が再燃したのは、アメリカ連邦捜査局（以下、「FBI」と略。）が 2015 年に 2 件の事案について、全令状法に基づき Apple 社に対し iPhone のロック機能解除を支援する命令を出すように連邦地方裁判所に求め、うち 1 件については FBI の求めに応じて連邦地方裁判所がロック機能解除支援を命じる命令を発出したことをきっかけとする。その後、FBI が命令を出すように求めた訴えを取り下げたため、2 件の事案自体はひとまず法的には終結している[44]。

38 United States v. New York Tel. Co., 434 U.S. 159 (1977).
39 Orin Kerr, *Preliminary Thoughts on the Apple iPhone Order in San Bernadino Case (Part 1)*, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/18/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-1/.
40 Application of United States, 427 F.2d 639 (9th Cir. Nev. 1970). 本件では、総合犯罪防止安全市街地法(Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.S. § 2518)に基づき政府が特定電話番号の電話盗聴の令状発給を求めると共に、電話会社に FBI に対して技術的支援を行うように命令することをネバダ連邦地裁に求めたが、連邦地裁はこれを退けた。連邦控訴裁も、連邦地裁の判断を支持した。
41 Application of United States for Order Authorizing Installation & Use of Pen Register, 546 F.2d 243 (8th Cir. Mo. 1976).
42 United States v. New York Tel. Co., 434 U.S. 159, 175 (1977).
43 Babington v. Yellow Taxi Corp., 250 N. Y. 14, 17, 164 N. E. 726, 727 (1928).
44 湯淺、前注 22。

4　おわりに

前述したように、連邦最高裁は、強制する内容に被疑者の知性が伴うか、それとも単なる肉体的行動であるかによって判断しており、「知性・肉体基準」とでも評すべき基準を用いている。

しかし人の知能の営為が関係するか、それとも単に肉体的な動作にすぎないかというこのような二分法が、今日における暗号化や認証に関する技術にも適合的であるかについては、疑問も残る。

たとえば、この基準を敷衍すれば、指紋認証や顔認証等のバイオメトリクス認証を利用して暗号化したりロックしたりしている場合には、当該の指紋等を提示させることで復号・ロック解除することが可能となるが、指紋や顔の提示の強制は身体を物理的に動作させることを強制するにとどまると解することも可能となる。このように解すれば、指紋認証や顔認証等により復号する際には必ずしも人の知能は必要としないから、尿の採取と同様であるということになり、憲法上の問題は生じないことになる。しかし、一般にバイオメトリクス認証は認証機能を強化するために用いられるものであり、バイオメトリクス情報自体も身体情報である点でセンシティブなものであるにもかかわらず、パスワードよりも憲法上の保護の度合いは低いということには、違和感が残る。もっとも、バイオメトリクス認証については、修正第 5 条の問題ではなくプライバシーの問題であると捉えることもできよう。

他方で、スマートフォンのロック等で多用されるようになっているパターンロックは、通常、画面上のいくつかの点の上をあらかじめ設定したパターン通りになぞってロック解除するというものであるが、これについては、おそらく金庫のダイヤル式の鍵を開けさせる場合と同様の扱いを受けると思われる。画面上のいくつかの点の上をあらかじめ設定したパターン通りになぞるには、指紋認証や顔認証等とは異なり、ダイヤルを回し鍵の組み合わせをして解錠するような仕組みの金庫のダイヤル式の鍵を開けさせるという場合と同様の知能の営為とその外的表現が必要とされる。そうだとすると、1988 年のド一対合衆国事件[45]が先例となり、あらかじめ設定したパターン通りになぞることの強制は憲法違反と判断される可能性が高いであろう。

またアメリカにおいては、iPhone のロック機能解除問題をきっかけとして、安全保障やテロ対策とプライバシーとの相克という観点から暗号化の是非をめぐる議論が始まっている。たとえばハーバード大学バークマン・インターネット及び社会センターは、"Don't Panic."と題するレポートを 2016 年 2 月に公開した[46]。これに対し政府の情報機関は、ワイデン連邦上院議員にレポート内容を批判する書簡を送付するなど[47]。暗号化に関する安全保障やテロ対策とプライバシーとの対立は、政治問題ともなってきている。さらに、2016 年 4 月 7 日、The Hill 誌が、連邦議会上院に超党派で暗号化されたデバイスに関する法案を提出する動きがあると報道し[48]、法案準備者と報道された連邦議会議員もそれを認めた。

今後、政府や捜査機関等がロックを解除したりデータを取り出したりすることができるようにあ

45 Doe v. United States, 487 U.S. 201, 210 (1988).
46 https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf
47 https://www.wyden.senate.gov/download/?id=3F716160-095E-420E-93F3-849453EB61B2&download=1
48 Cory Bennett, *Senate Encryption Bill Draft Mandates 'Technical Assistance'*, THE HILL, April 7, 2016, http://thehill.com/policy/cybersecurity/275567-senate-intel-encryption-bill-mandates-technical-assistance.

らかじめ製品を設計することを義務づけたり、ロック機能自体を禁止したりする連邦法の制定に向けた動きが活発化する可能性がある。このような法律が制定されれば、本件で問題となっているような被疑者への暗号の復号（暗号化の解除）の強制の必要性は低くなるであろう。しかし、それは他の憲法上の権利を侵害する危険性はないのであろうか。また、憲法に違反するとすれば、それは何条に違反するのかという点での議論も生じると思われる。

5　謝辞

本稿は、平成 26 年度科学研究費補助金基盤研究（C）「行政におけるデータの取扱いに関する法的規制の比較研究」（課題番号 26380153）及び CREST・さきがけ複合領域「ビッグデータ統合利活用のための次世代基盤技術の創出・体系化」平成 27 年度採択課題「ビッグデータ統合利用のためのセキュアなコンテンツ共有・流通基盤の構築」（研究代表：山名早人）の研究成果の一部である。