デジタル時代のアメリカ自己負罪拒否特権

――デジタルデバイスのロック解除と自己負罪拒否特権に関する一考察――

梶　　悠輝

Ⅰ　はじめに

日本国憲法38条１項は、「何人も、自己に不利益な供述を強要されない」と規定し、いわゆる自己負罪拒否特権を保障している。この自己負罪拒否特権により強要から保護される「供述」には、文字通りの口頭供述のみならず、文書も含まれる[1)]。また、手話や指差し、首肯といった、「コミュニケーション的」な側面をもつ動作や挙動も含まれる[2)]。

その一方で、指紋・足形の採取、身体の測定や写真の撮影、身体検査といった身体的特徴に関する情報の取得は、「供述」の強要には当たらず、もっ

1)　奥平康弘『憲法』（第３巻、有斐閣、1993）353頁。
2)　渋谷秀樹『憲法』（第３版、有斐閣、2017）246頁、樋口陽一＝佐藤幸治＝中村睦男＝浦部法穂編『憲法』（第２巻、青林書院、1994）［佐藤幸治］363頁。

ぱら令状主義を保障する憲法35条[3]の規律対象となると解されてきた[4]。そのため、令状主義の要求を満たす限りにおいて、捜査機関は、身体的特徴に関する情報を強制的に取得することができる。

この点は、日本国憲法38条１項の母法であり、「何人も、刑事事件において、自己に不利益な証人になるよう強要されない」と規定する合衆国憲法修正５条を擁するアメリカ合衆国でも同様である。修正５条の保護が発動する要件は、①強要の対象が、刑事手続上、自己に「不利益」なものであること、②その対象が「供述」であること、③「強要」が存在することである。これら３つの要件がすべて満たされれば、当該供述は修正５条により強要から保護される。このうち②の「供述」要件に関し、合衆国最高裁は、人物特定に際して、特定の衣服の着用[5]、血液サンプルや指紋の提供[6]、面通しでの整列[7]、

3）　１項「何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第33条の場合を除いては、正当な理由に基いて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない」。２項「捜索又は押収は、権限を有する司法官憲が発する各別の令状により、これを行ふ」。

4）　「コミュニケーション的」側面のない証拠が「供述」に含まれないことを明確に論じた邦語文献として、酒巻匡『刑事訴訟法』（第２版、有斐閣、2020）190頁、佐藤幸治『日本国憲法論』（第２版、成文堂、2020）382頁、鈴木茂嗣「自己負罪供述強要の禁止」樋口陽一＝佐藤幸治編『憲法の基礎』（青林書院、1975）378頁以下、379頁、田宮裕「被告人・被疑者の黙秘権」日本刑法学会編『刑事訴訟法講座』（第１巻、有斐閣、1963）79-80頁。笹倉宏紀「自己負罪拒否特権」法学教室265号（2002）103頁以下、107-108頁も参照。なお、最判平成９年１月30日刑集51巻１号335頁において、最高裁は、道路交通法上の呼気検査拒否罪について、呼気検査が「運転者らから呼気を採取してアルコール保有の程度を調査するものであって、その供述を得ようとするものではない」点を理由に、憲法38条１項に違反しないとした。同判決の調査官解説は、その趣旨について、呼気検査があくまで呼気という「物的」・「非供述的」な証拠の採取である点に合憲性の根本的な理由があると説明し、自己負罪拒否特権の保護対象が「供述」に限られるとする見解が通説であるとする。三好幹夫「判解」『最高裁判所判例解説刑事篇（平成９年度）』（法曹会、1998）42頁以下、54頁。他方で、かつて、「供述」には自己に不利益な内容をもつ「物」の提供も含まれると解するべきであると明確に論じた数少ない見解として、伊藤正己『憲法』（第３版、弘文堂、1995）349頁。

5）　Holt v. United States, 218 U.S. 245 (1910).

6）　Schmerber v. California, 384 U.S. 757 (1966).

7）　United States v. Wade, 388 U.S. 218 (1967).

筆跡の提供[8]、声紋の提供[9]について、いずれも「供述」該当性を否定してきた。

このように身体的特徴の開示について「供述」該当性を否定してきた合衆国最高裁の姿勢は、その判示に表れている。例えば、特定の衣服の着用が問題となった1910年ホルト・ケース合衆国最高裁判決の「（自己負罪強要の）禁止は、その者からコミュニケーションを強要するために物理的または道徳的強制力を用いることの禁止であり、同人の身体的特徴が重要である場合に、証拠としてのそれを排除すべきとするものではない[10]」との判示や、血液サンプルや指紋の提供が問題となった1966年シュマーバー・ケース合衆国最高裁判決の「…（自己負罪拒否）特権は、被告人が自己に不利益な証言を行うこと、または供述的もしくはコミュニケーション的性質を帯びる証拠を州に提供することの強制からのみ保護される…[11]」との判示である。

こうした合衆国最高裁の姿勢は、金庫の「鍵」と壁掛け金庫の「番号」のアナロジーで説明される[12]。すなわち、物理的に存在する金庫の「鍵」の明渡し（surrender）は「供述」ではなく、したがって、不合理な捜索押収を禁止する修正４条[13]のみによって保護される一方、壁掛け金庫の「番号」の提供（giving）は「供述」に該当し、したがって修正５条の保護を受けることになるというわけである。このアナロジーに従い、人物特定のために開示を強制された身体的特徴は、壁掛け金庫の「番号」の伝達のような「供述的」・「コミュニケーション的」性質は認められず、物理的に存在する金庫の「鍵」に近いとされてきた。

近時、アメリカでは、「供述」要件との関係で、スマートフォンを含む携帯電話等のデジタルデバイスのロックの解除を強制することが自己負罪拒否

8）　Gilbert v. California, 388 U.S. 263 (1967).
9）　United States v. Dionisio, 410 U.S. 1 (1973).
10）　Holt (n.5).
11）　Schmerber (n.6).
12）　Doe v. United States, 487 U.S. 201, 219 (1988) (Steven J., dissenting).
13）　U.S. Const. amend. IV.「不合理な捜索及び…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」。

特権侵害に当たるのかが、「裁判所や研究者を悩ませる根本的な問題[14]」、「デジタル時代における自己負罪拒否特権の最も重要な問題[15]」として顕在化してきた[16]。現在、多くのデバイスにロックがかけられるのが一般的になり、さらに、ロック時にコンテンツが「暗号化」される機種も普及している[17]。ここにいう「暗号化」とは、デバイスの中身を解読不能な文字列にすることを指し、「暗号化」が施されたデバイスについては、ロックを解除して「復号」しなければ、その中身が判読できなくなる。しかも、暗号の解析が容易でないケースも少なくない[18]。このため、捜査官には、被疑者本人にロックを解除させたいというインセンティブが働くのである[19]。

14）　Laurent Sacharoff, Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 203, 207 (2018).

15）　David Rangaviz, Compelled Decryption & State Constitutional Protection against Self-Incrimination, 57 Am. Crim. L. Rev. 157, 157 (2020).

16）　すでに日本でも、急速なコンピュータの普及等を理由に、捜索差押のような対象者にその権利の制約を受忍するよう強制する強制処分と、刑訴法221条の領置のような対象者の任意の協力を得て行われる任意処分との中間的な処分として、対象者に被疑者をも含めた提出命令制度の必要性が指摘されている。酒巻匡「新しい証拠収集手段」ジュリスト1228号（2002）125頁以下。また、暗号解除に関わる法制度の設計を検討することが強く求められる現状を念頭に、日本国憲法38条の保障範囲を明らかにする必要性を説く邦語文献として、丸橋昌太郎「黙秘権と自己負罪拒否特権の意義について」秋吉淳一郎＝木村光江＝川田宏一＝星周一郎＝細谷泰暢編『これからの刑事司法の在り方：池田修先生 前田雅英先生退職記念論文集』（弘文堂、2020）172頁以下。なお、イギリスにおけるデジタルデバイスと自己負罪拒否特権の関係を論じた邦語文献として、同「暗号解除に関する規律について」『日高義博先生古稀祝賀論文集』（下巻、成文堂、2018）393頁以下。加えて、英米におけるパスワードによるロック解除と自己負罪拒否特権に関して詳細に整理し検討を行った近時の邦語文献として、山田峻悠「自己負罪拒否特権の『対象』に関する検討（１～２・完）」法学会雑誌62巻１号（2021）447頁以下、同２号（2022）275頁以下を参照。

17）　デジタルデバイスのロック解除と犯罪捜査に関しては、2015年にアメリカのカリフォルニア州で発生した銃乱射事件において、FBI（連邦捜査局）が、iPhone を販売する Apple 社に対して、捜査の過程で押収された iPhone のロックの解除を命じるよう連邦地裁に請求したことに端を発する「Apple 対 FBI 問題」が知られている。この事件については、指宿信「Apple 対 FBI 問題」同『電脳空間と刑事手続』（成文堂、2022）179頁以下。

18）　Orin Kerr and Bruce Schneier, Encryption Workarounds, 106 Geo. LJ 989, 1011 (2017) は、当局が暗号化を確実に回避できる「魔法のような」方法は一つもないと指摘する。

19）　経済的・時間的コストの面でも、捜査官が本人にロック解除を求めるインセンティブが働く。See, Carissa Uresk, Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement, 46 BYU L. Rev. 601 (2021) Ch.I.

デバイスのロックの種類は、一般に、パスワードによるものと、指紋認証や顔認証といった生体認証によるものがある。パスワードでロックされている場合、解除を強制する方法として、「文書提出命令（Subpoena Duces Tecum）」により、パスワードの開示や入力、復号済みのデバイスやそのコンテンツの提出を求める方法がある。文書提出命令とは、証人に対して、法廷侮辱の制裁による威迫のもと、事件に関連する文書等の提出を命じるものを指す[20]。生体認証でロックされている場合、警察の捜査段階においては、あらかじめ捜索令状等を取得したうえで、指紋や容貌等の生体情報を物理的に提示させる方法がある。

もっとも、生体認証の場合、ロック解除のために利用される指紋や容貌等の生体情報は身体的特徴である。そのため、身体的特徴の開示に関する合衆国最高裁の姿勢に照らせば、一見すると、生体情報の提供は金庫の「鍵」の明渡しであり、その提供を強制することに修正５条の問題は生じないように思われる。しかし、実際には、後述の通り、生体認証への修正５条の適用の適否に関して、下級審の裁判所の立場は一致していない。生体認証に修正５条の適用を認める立場の背景には、近時の携帯電話と犯罪捜査に関する2014年ライリー・ケース合衆国最高裁判決[21]、および2018年カーペンター・ケース合衆国最高裁判決[22]がある。とりわけ前者は、生体認証の文脈において、判決文や論文の中で頻繁に引用されている。2014年ライリー・ケース合衆国最高裁判決では、警察官が、適法な逮捕に伴う無令状捜索が許される状況において、被疑者の携帯電話の中身に対して無令状で行った捜索が、修正４条

20）　アメリカでは、連邦の経済犯罪や組織犯罪を中心に、起訴相当かどうかを審査する大陪審による提出命令が用いられることがあるとされる。酒巻匡「アメリカにおける自己負罪拒否特権の一断面」廣瀬健二＝多田辰也編『田宮裕博士追悼論集』（下巻、信山社、2003）447頁以下、447-448頁。

21）　Riley v. California, 573 U.S. 373 (2014).

22）　Carpenter v. United States, 138 S. Ct. 2206 (2018). 携帯電話基地局が保管する被疑者の位置情報に「第三者法理」は適用されないとした判例である。「第三者法理」とは、個人が自発的に第三者に提供した情報は修正４条の保護を受けないとする理論を指す。同判決については、拙稿「アメリカ合衆国における『ごみ捜査』同志社法学74巻１号（2022）545頁以下、576頁以下を参照。

の禁止する不合理な捜索押収に当たると判示された。その中で、最高裁は、「（携帯電話は、）火星からの訪問者が、人体構造の重要な特徴であると結論づけるかもしれないほど、日常生活に深く浸透した[23]」と指摘したうえで、「現代の技術により、個人がその手に…情報を持ち運べるようになったからといって、その情報について、建国者たちが勝ち取った保護を受けるに値しなくなるわけではない[24]」と説示している。これらの説示が、デジタルデバイス、とりわけ携帯デバイスを「内心（や人体）の拡張」の一環と捉えて特別な配慮を求めるものなのか、あるいは単なるリップサービスなのかは判然としない。いずれにせよ、両判決は、生体認証の解除の強制と自己負罪拒否特権を巡る議論に影響を及ぼさずにおかない[25]。

以上の背景のもと、本稿では、自己負罪拒否特権の「供述」概念の内実や、デジタル時代における自己負罪拒否特権の適正な保障範囲を明らかにするうえでの有益な示唆を得るため、文書提出命令[26]の文脈で形成された文書と自己負罪拒否特権に関する合衆国最高裁の先例を概観したうえで（Ⅱ）、まずは、パスワードによるロック解除と自己負罪拒否特権に関する判例や議論について（Ⅲ）、次に、生体認証によるロック解除と自己負罪拒否特権に関する判例や議論について（Ⅳ）整理し、若干の考察を行うことにしたい（Ⅴ）。

23）　Riley (n.21), at 385.

24）　*Id.*, at 403.

25）　See, Joey Blanch and Stephanie Christensen, Biometric Basics: Options to Gather Data from Digital Devices Locked by a Biometric Key, 66 Dep't of Just. J. Fed. L. & Prac. 3, 6-7 (2018). 同論文は、カリフォルニア州中央地区合衆国検事局暴力・組織犯罪課副課長を務めるジョーイ＝ブランチと、同局コンピュータ犯罪・知的財産課課長を務めるステファニー＝クリステンセンの共著によるものである。生体認証の解除強制と自己負罪拒否特権の問題について、ライリー・ケース合衆国最高裁判決をあげたうえで、検察当局として、一部の裁判官の中にある「携帯電話は特別」との議論に注意する必要があると指摘する。

26）　日本には文書提出命令に相当する制度はなく、そのため、ここでの議論は日本法のもとで争点となりうるものではない。しかし、酒巻・前掲注（20）448頁では、「彼地における自己負罪拒否特権の機能の一局面を紹介し、特権の適用範囲について考察を深める」目的で、文書提出命令と自己負罪拒否特権の関係が論じられている。本研究もこれに倣うものである。

Ⅱ　文書と自己負罪拒否特権に関する合衆国最高裁判例

前述の通り、捜査機関が、デジタルデバイスのロックの解除や復号されたデバイスの提出を被疑者に求める場合、「文書提出命令」が活用されている。そこで、本章では、デジタルデバイスに対する文書提出命令の活用の前提として、自己負罪拒否特権が文書に及ぶことを確認した1886年ボイド・ケース合衆国最高裁判決[27]と、後に見るように、その論理を修正した1976年フィッシャー・ケース合衆国最高裁判決[28]に焦点を当て、判例の展開を概観する。

1　1886年ボイド・ケース合衆国最高裁判決

（1）本判決の意義　1886年ボイド・ケース合衆国最高裁判決[29]は、自己負罪拒否特権の保障範囲を口頭の供述から文書に拡大し、かつ文書の内容の自己負罪的な性格を理由に、当該文書は修正５条で保護されることを明らかにしたものである[30]。

27）　Boyd v. United States, 116 U.S. 616（1886）.

28）　Fisher v. United States, 425 U.S. 391（1976）.

29）　Boyd（n.27）. 本判決に関する邦語文献として、酒巻・前掲注（20）、安井哲章「合衆国憲法第五修正の自己負罪拒否特権の誕生」法学新報127巻９＝10号（2021）83頁以下。

30）　Richard Nagareda, Compulsion to Be a Witness and the Resurrection of Boyd, 74 NYUL Rev. 1575, 1578（1999）; Samuel Alito Jr., Documents and the Privilege Against Self-Incrimination, 48 U. Pitt. l. Rev. 27, 29（1986）; Heidt Robert, The Fifth Amendment Privilege and Documents-Cutting Fisher's Tangled Line, 49 Mo. L. Rev. 439, 444（1984）; Robert Gerstein, The Demise of Boyd: Self-Incrimination and Private Papers in the Burger Court, 27 UCLA L. Rev. 343, 362（1979）; Georganne Higgins, Business Records and the Fifth Amendment Right Against Self-Incrimination, 38 Ohio St. LJ 351, 352-353（1977）; Mark Berger, The Unprivileged Status of the Fifth Amendment Privilege, 15 Am. Crim. L. Rev. 191, 219（1977）; Ted Pitts, Fifth Amendment Interpretation in Recent Tax Record Production Cases, 46 U. Cin. L. Rev. 232, 233（1977）; Henry Friendly, The Fifth Amendment Tomorrow: The Case for Constitutional Change, 37 U. Cin. L. Rev. 671, 682（1968）; Herschiel Barnes and Charles Cosner, To What Extent Does the Privilege against Self-Incrimination Protect a Witness against Forced Production of Documents, 1 Vand. L. Rev. 626, 627-628（1947）; J. Grant, Constitutional Basis of the Rule Forbidding the Use of Illegaly Seized Evidence, 15 S. Cal. L. Rev. 60, 61（1941）.

（2）**事実概要**　本件は、1874年６月22日に可決された「関税歳入法を改正する法律」の第12条に基づく板ガラス35ケースに対する財産の押収および没収手続に関するものである。同条は、輸入荷物の所有者、輸入者、荷受人等が、不正や虚偽の請求書等の書面や供述により関税を詐取し、または詐取する意図で行った輸入（未遂も含む）等に対して、50ドル以上5,000ドル以下の罰金刑もしくは２年以下の拘禁刑、またはその両方を科すとともに、当該商品の没収を規定していた。

原審[31]の認定によると、政府は以前、フィラデルフィアの裁判所および郵便局の建設に利用するために、被告人から大量の板ガラスを、国内価格から関税率分を割引した価格で調達した。これは、被告人が、政府に供給した板ガラスに代え、同量の新しいガラスを関税無しで輸入してよいとの契約に基づいていた。ところが、被告人は、虚偽の書簡や不正な書類を使用して財務長官代理に免税許可証を発行させ、政府に供給した量をはるかに超えるガラスを、関税を免れて輸入しようとした。35ケースのガラスが港に到着すると、被告人のブローカーは、前記の免税許可証をニューヨークの税関に提出した。しかし、ガラスの引き渡しは中止され、「関税歳入法を改正する法律」の第12条に基づき、被告人は、同条違反および詐欺の罪で訴追され、35ケースのガラスは没収のために押収された。

正式事実審理の過程で、本件で押収された35ケースに先立ち輸入されていた29ケース分のガラスの量と価格を示すことが重要になった。そのため、ニューヨーク地区連邦検事局の検事は、「関税歳入法を改正する法律」の第５条に基づき、当該29ケースに関するインボイスを提出するよう命令を発した。同条には、領収書等の提出命令や当局による保管に関する規定に加え、提出が行われなかった際には、対象者が自白したものとみなす規定が定められていた。被告人は、命令に従いインボイスを提出したが、その手続の中で、没

31）　United States v. Boyd, 24 F. 690 (S.D.N.Y. 1885) and United States v. Boyd, 24 F. 692 (S.D.N.Y. 1885). 前者は、1874年６月22日に可決された「関税歳入法を改正する法律」の第12条に基づく没収手続であり、後者は同条に基づく刑事事件である。

収の有効性への疑義や、対象者に対して自己に不利益な証拠の提出を強要することにかかる憲法上の疑義を理由に、当該インボイスの証拠排除を主張した。

正式審理では、被告人らによる証拠排除の主張は認められず、陪審は没収を認める評決に至った。この評決は合衆国第２巡回区控訴裁判所でも是認されたが、合衆国最高裁は、本件の争点が市民の安全や特権、免責にかかわる憲法上の重大性な問題であることに鑑み、原判決を審査することにした。

(3) 判　旨　まず、合衆国最高裁は、修正４条との関係で、本件の文書提出が個人の家に無理矢理侵入して書類を調べるような、事実上の捜索押収ではないとしつつ、「関税歳入法を改正する法律」における自白のみなしに関する規定と、同法の目的が、対象者から自己に不利益な証拠を強制的に取得することにある点を理由に、提出命令の対象の私文書には修正４条の保護が及びうるとの見解を示した[32]。そのうえで、私的な書類は個人のかけがえのない私有財産であるとし[33]、個人に対して私文書の提出を強制することで同人を有罪にしたり、同人の物品を没収したりするための証拠として使用したりすることは、修正４条に違反すると説き、修正４条と修正５条の保障範囲はほとんど競合するとの見方を示した[34]。

次に、修正５条との関係では、同条と修正４条との密接な結びつきを確認しつつ、不合理な捜索押収の目的が、ほとんどの場合、対象者に対して自己に不利益な証拠を提出させる目的で行われ、したがって両者に実質的な差異

32)　Boyd (n.27), at 621-622.

33)　*Id.*, at 627-628. 合衆国最高裁は、私的な書類の保護を論じるにあたり、Entick v. Carrington, 19 Howell's State Trials 1029 (1765) に依拠した。この判決は、国王の名誉を毀損した容疑の証拠を収集するために、対象者の自宅の書類等を無差別に捜索押収することを許容する一般令状の慣行が残っていた18世紀後半のイングランドにおいて、当局による原告の住居への侵入や、机や箱等の破壊、書類の捜索が、コモンロー上の不法侵入に該当するかどうかが争われた事件に関するものである。なお、同判決の原典に当たることができなかったため、井上正仁『強制捜査と任意捜査』（新版、有斐閣、2014）45頁、およびそこに引用されている William Cuddihy, The Fourth Amendment : Origins and Original Meaning, 602-1791, 593-594 (2009) による要約を参照した。

34)　Boyd (n.27), at 630.

は認められないと論じたうえで、財産を没収する目的で行われる訴訟手続は形式的には非刑事手続であっても、本質的には刑事手続であると判示した[35]。

以上を踏まえ、最高裁は、結論として、本件インボイスの提出を求める通知、その裏づけとなった命令や法律の違憲無効を認め、控訴裁判所判決を破棄して差し戻した。

2　1976年フィッシャー・ケース合衆国最高裁判決

（1）本判決の意義　1976年フィッシャー・ケース合衆国最高裁判決[36]の背景には、プライバシーを介して修正４条と修正５条を組み合わせることで、自己に不利益になりうる私文書への提出命令が両条項に違反するとした前記のボイド・ケース合衆国最高裁判決の論理[37]への疑問があった。すなわち、両条項を混同しているとの疑問[38]や、その論理に従えば、犯罪の嫌疑のある者について、財産権を理由にその財産を捜査することがおよそ許されなくなるという不合理な帰結を招きうるとの疑問[39]である[40]。そこに本判決が登場し、後に詳述する「提出行為（the act of production）」の法理と「自明の帰結（the foregone conclusion）」法理を生み出し、ボイド・ケース合衆

35）　*Id.*, at 633-634.

36）　Fisher（n.28）. 本判決に関する邦語文献として、酒巻・前掲注（20）、鈴木義男編『アメリカ刑事判例研究』（第１巻、成文堂、1982）53頁以下［神坂尚］、安井哲章「自己負罪拒否特権と文書提出命令（１）」法学新報111巻１＝２号（2004）299頁以下、307頁以下。

37）　Leonard Ratner, Consequences of Exercising the Privilege Against Self-Incrimination, 24.3 The University of Chicago Law Review 472, 486, 488（1957）; Thomas Hendrix, Recent United States Supreme Court Interpretations of the Law of Searches and Seizures, 37.5 Journal of Criminal Law and Criminology 413, 418（1947）; Leonard Martin, Investigatory Powers of Congress and Administrative Agencies, 26 Wash. ULQ 531, 538（1940）.

38）　Alito Jr., *supra* note 30, at 36; Gerstein, *supra* note 30, at 344, 363-365. 安井・前掲注（36）320頁も参照。

39）　Robert Heidt, The Fifth Amendment Privilege and Documents-Cutting Fisher's Tangled Line, 49 Mo. L. Rev. 439, 444（1984）. 酒巻・前掲注（20）451頁も参照。

40）　ただし、ボイド・ケース合衆国最高裁判決は、アメリカ合衆国における市民の自由にとって記念碑的な判例として称賛されてきた点には留意を要する。安井・前掲注（29）104頁。See also, Olmstead v. United States, 277 U.S. 438（Brandeis, J., dissenting）.

国最高裁判決を修正するに至った。

⑵　事実概要　本件は、連邦所得税法違反を被疑事実とする２つの事件（以下、フィッシャー事件およびカスミール事件）に関するものであり、本件審査は、それぞれの事件に関して、IRS（内国歳入庁）の調査官が調査のために行った文書提出命令の強制執行の申し立てに関するものである。両事件に共通する事実関係は次のとおりである。税務調査の対象となった納税者は、会計士の作成した確定申告書に関わる一切の文書を会計士から入手し、当該文書を弁護士のもとに移した。その後、文書の所在を把握したIRSは、弁護士に対し、文書の提出を求める召喚状を送達したところ、弁護士はこれに応じなかった。そこで、当局は、連邦地裁による召喚状の執行命令を受けて、強制執行を行った。両事件の弁護士は、各命令について控訴裁判所に上訴した。

フィッシャー事件において、弁護士および納税者は、合衆国憲法修正４条および修正５条違反に加え、依頼者・会計士・弁護士間の秘匿特権の侵害を主張した[41]。合衆国第３巡回区控訴裁判所は、納税者が文書の所有権を取得していたことはなく、弁護士の手元にある文書は提出を免れないとして、地裁の命令を是認した。

他方で、カスミール事件では、弁護士は、修正５条および修正４条違反に加え、依頼者・弁護士間の秘匿特権の侵害を主張した。合衆国第５巡回区控訴裁判所は、納税者が文書を所有していた場合、納税者は、自身に向けられた召喚状による提出について、修正５条の特権を享受することができるとした。加えて、弁護士・依頼者間の関係に照らしても、納税者は、文書を弁護士に移した後も、文書に対する特権を維持していたとして、文書の提出を命じた地裁の命令を破棄した。

⑶　判　旨　両控訴審判決の対立を受けて、最高裁は、まず、本件書類

41）　なお、弁護士は、形式的には修正５条違反のみを主張していたが、召喚状の執行が、とりわけ弁護士とのコミュニケーションの秘匿性に照らし、納税者のプライバシーに対する「合理的な期待」の侵害を伴う点を根拠にしており、実質的には修正４条違反を主張していたものと捉えられた。Fisher（n.28）, at 1573.

の提出命令が納税者に対する供述の「強要」に該当するかについて、訴追の対象となっているのは弁護士ではなく納税者であり、弁護士が納税者の代理人であるか否かにかかわらず、本件提出命令は納税者に対する供述の「強要」には当たらないとした[42]。

また、修正４条と修正５条の関係について、供述の「強要」を伴わずに取得された証拠には修正５条が適用されず、修正４条による規律が問題となるとした[43]。そして、相当な理由により制約が許されるプライバシーを保護する修正４条と、制約が許されない修正５条との性質の違いを説明したうえで[44]、その違いに照らし、修正５条の解釈において、「供述」の文理を重視し、修正４条で保障される一般的なプライバシーを加味しない姿勢を示した[45]。

以上を踏まえ、最高裁は、依頼人・弁護士間の秘匿特権の問題を論じた。まず、最高裁は、「依頼人により、法的支援を得るために行われた弁護士への秘密の開示は、特権として扱われる[46]」ことを認めつつ、本件の各納税者も、法的支援を得るために本件書類を弁護士に移管したと認定した。そのうえで、修正５条は、「被告人が、自己に不利益になる供述的なコミュニケーションを強要された場合[47]」にのみ適用されることを確認したうえで、残る問題として、本件文書が自己負罪拒否特権により保護される「供述」に該当するのかどうかを検討した[48]。

最高裁は、①本件提出命令で強要されるのは口頭の供述ではなく、②納税者自身に文書の内容について供述させるものでもなく、③本件書類は納税者ではなく会計士が作成したものであるため、納税者自身の供述的な意思表示も含まれていない点を指摘し、本件提出命令が直ちに修正５条に違反すると

42) *Id.*, at 1574.
43) *Id.*, at 1575.
44) *Id.*, at 1576.
45) *Id.*, at 1576.
46) *Id.*, at 1577.
47) *Id.*, at 1580.
48) *Id.*, at 1578.

はいえないとした[49]。その一方で、「…召喚に応じて証拠を提出するという行為（The act of producing evidence）は、提出された書類の内容とは全く独立して、それ自体コミュニケーション的な側面を有する。召喚状に従うことは、要求された書類が存在し、納税者がそれを所有または管理している事実を黙認することになる。また、その書類が召喚状に記載されているものであると納税者が知っている事実を示すものでもある[50]」と述べ、文書を含む証拠の提出行為それ自体が、「供述的」な性質をもちうる可能性を指摘した。

もっとも、本件書類は会計士が作成したものであり、会計士が顧客の税務申告に携わる際に一般的に作成されるものにすぎないことに照らし、最高裁は、「本件書類の存在と所在は自明の帰結（foregone conclusion）であり、納税者が書類を実際に所持している事実を認めることで、当局の情報の総和にほとんど何も付け加えることはない[51]」と論じ、本件提出行為は「供述」の問題ではなく「明け渡し」の問題であるとして[52]、本件提出命令は修正５条に違反しないと結論づけた。

３　「提出行為」の法理・「自明の帰結」法理と両判決以降の判例

以上の通り、フィッシャー・ケース合衆国最高裁判決は、前記のボイド・ケース合衆国最高裁判決が示した自己負罪拒否特権とプライバシーを同視する論理と、自己負罪的な内容の文書が修正５条により保護されるとの理解を修正し、提出行為の「供述」性の判断から、文書の内容の自己負罪的な性格を切り離して、提出行為から示唆される「供述」の有無を考えなければならないことを明らかにした[53]。これが、「提出行為」の法理である。この法理は、

49）　*Id.*, at 1580.

50）　*Id.*, at 1581.

51）　*Id.*, at 1581.

52）　*Id.*, at 1581.

53）　Nagareda, *supra* note 30, at 1578, 1590, 1594; Alito Jr., *supra* note 30, at 29, 31, 44; Heidt Rober, The Fifth Amendment Privilege and Documents-Cutting Fisher's Tangled Line, 49 Mo. L. Rev. 439, 470, 476（1984）; Paul Lipton, The Erosion of Constitutional Privileges, 23 Ann. Tax Conf. 29, 30, 34, 35（1977）; Berger, *supra* note 30, at 219–221.

強制された行為が修正５条にいう「供述的」かどうかを判断するための理論であり、当該行為が「コミュニケーション的側面」をもつ「暗黙の言明（tacit averment）」を示唆する場合、言い換えれば、何らかの事実を暗示する場合、当該行為は「供述的」性質を帯びるとする理論である[54]。この法理に従い、当該行為の「供述的」性質が認められた場合、その行為が「強要」され、そこから示唆される事実が被疑者にとって「不利益」なものであれば、当該供述は原則として修正５条の保護を受けることになる。

他方で、フィッシャー・ケース合衆国最高裁判決はもう１つ、「自明の帰結」法理を生み出した。この法理は、「提出行為」の法理の例外であり、当局がすでに知っているとあらかじめ立証した事実に照らして、強制された提出行為の「供述的」側面が当局のもつ情報の総和にほとんど、または全く何も加えないと認められる場合には、当該提出行為は強要された供述には該当しないとする法理である[55]。

両判決以降、まず、郡および地方自治体との契約に関する汚職の被疑事実について、大陪審が発した文書提出命令の是非が争われた1984年ドゥー・ケース合衆国最高裁判決[56]において、前記のフィッシャー・ケース合衆国最高裁判決が示した論理が再確認された[57]。さらに、被告人が税法違反および詐欺の罪に問われた事件に関し、被告人が大陪審による文書提出命令のもとで証言を強要されたことが修正５条に違反するかどうかが争われた2000年ハッベル・ケース合衆国最高裁判決[58]では、「自明の帰結」法理の適用に際し、当局があらかじめ立証しておくことが求められるその立証の程度として、「合

54）　Orin Kerr, Compelled Decryption and the Privilege against Self-Incrimination, 97 Tex. L. Rev. 767, 772 (2018).

55）　Kerr, *supra* note 54, at 773.

56）　Doe v. United States, 465 U.S. 605 (1984). 本判決に関する邦語文献として、安井・前掲注（36）311頁以下、酒巻・前掲注（20）454-455頁、田村泰敏「判批」渥美東洋編『米国刑事法の動向Ⅰ』（中央大学出版部、1989）197頁以下。

57）　Alito Jr., *supra* note 30, at 29.

58）　United States v. Hubbell, 530 U.S. 27 (2000). 本判決に関する邦語文献として、麻妻みちる「判批」堤和道編著『米国刑事判例の動向』（中央大学出版部、2022）513頁以下、安井哲章「自己負罪拒否特権と文書提出命令（４・完）」法学新報111巻11=12号（2005）231頁以下。

理的な具体性（reasonable particularity）」が求められることが確認され、その適用基準の明確化が図られた[59]。

Ⅲ　パスワードによるデバイスのロック解除と自己負罪拒否特権

Ⅰで述べたように、近年、スマートフォンを含む携帯電話等のデジタルデバイスが普及し、それらにパスワードや生体認証によるロックがかけられるとともに、ロックによりその中身が暗号化されているケースが一般的になっている。こうした実情を背景に、捜査機関が、「提出命令」を通じて、被疑者に対し、そのデバイスのパスワードや復号されたデバイスの提出を強制する事例が見られるようになり、この提出行為の強制が合衆国憲法修正５条にいう「供述」の強要に当たり、自己負罪拒否特権に違反するのかどうかについて、議論が戦わされている。

2022年11月現在、デジタルデバイスのパスワードや復号されたデバイスの提出を強制することが自己負罪拒否特権侵害に該当するかどうかについて判断を下した合衆国最高裁判例は見られない。連邦や州の下級審では、パスワードによるロック解除の強制は「内心」の開示にあたるため、「供述的」性質が認められるとするものがほとんどである[60]。もっとも、提出行為自体に

59）　Jason Wareham, Cracking the Code: The Enigma of the Self-Incrimination Clause and Compulsory Decryption of Encrypted Media, 1 GEO. L. TECH. REV. 247, 255 (2017).

60）　Uresk, *supra* note 19, at 621; Ariel Redfern, Face It-The Convenience of a Biometric Password May Mean Forfeiting Your Fifth Amendment Rights, 125 Penn St. L. Rev. 597, 614 (2020); Nathan Reitinger, Faces and Fingers: Authentication, 20 J. High Tech. L. 61, 63 (2020); Adam Herrera, Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free From Self-Incrimination, 66 UCLA L. Rev. 778, 798 (2019); Pratik Parikh, IPHONE X: Unlocking the Self Incrimination Clause of the Fifth Amendment, 45 Rutgers Computer & Tech. LJ 58, 79, 87 (2019); Aloni Cohen and Sunoo Park, Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries, 32 Harv. JL & Tech. 169, 184 (2018); Efren Lemus, When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones, 70 SMUL Rev. 533, 553 (2017); Jeffrey Kiok, Missing The Metaphor: Compulsory Decryption and the Fifth Amendment, 24 BU Pub. Int. LJ 53, 65 (2015).

「供述的」性質が認められるとしても、文書の提出の場合と同様、提出行為により暗示される事実が「自明の帰結」と認められる場合、その提出の強制が許容されることになる。この「自明の帰結」法理に関して、裁判所の立場は、その適用に際し、当局によりあらかじめ、①被疑者が媒体の「パスワードを知っている」事実が立証されていれば足りるのか、②それを超えて、当局がデバイスの内容に関する知識を有している事実を立証することまで求められるのかで分かれている[61]。

そこで、本章では、パスワードでロックされたデバイスを念頭に、「自明の帰結」法理の適用に当たり対照的な姿勢を示した２つの代表的な判例に焦点を当てる[62]。次に、被疑者にパスワードの提出やパスワードでロックされたデバイスの復号を強制することが自己負罪拒否特権侵害にあたるのかどうかを巡る議論状況を整理する。

1　代表判例

（1）2018年スペンサー・ケースカリフォルニア州北部地区連邦地方裁判所判決　まず、「自明の帰結」法理の適用に際して、「①被疑者が媒体のパスワードを知っている事実が立証されていれば足りる」との姿勢を示した代表的[63]な判例として、2018年スペンサー・ケースカリフォルニア州北部地

61）　Uresk, *supra* note 19, at 621–622.

62）　本稿では、Kerr, *supra* note 54, at 769, n.7で対置されている２つの判例を代表判例として抽出した。筆者のオリン・カー教授は、合衆国憲法修正４条および刑事訴訟法研究の第一人者として知られ、コンピュータ犯罪や電子証拠と法理論に関して多くの業績をもち、その多くが判決文に引用されるなど、アメリカで最も影響力のある法学研究者の１人である。なお、同論文（*Id.*, n.4）には、この論点を扱った近時の判例として、他に以下のものが列挙されている。United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012); Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014); State v. Stahl, 206 So. 3d 124 (Fla. Dist. Ct. App. 2016); United States v. Apple MacPro Comput., 851 F.3d 238 (3d Cir. 2017); United States v. Mitchell II, 76 M.J. 413 (C.A.A.F. 2017); Seo v. State, 109 N.E.3d 418 (Ind. Ct. App.), transfer granted, opinion vacated, 119 N.E.3d 90 (Ind. 2018).

63）　Kerr, *supra* note 54, at 769, n.7. 本判決を「自明の帰結」法理の適用にあたり「被疑者が媒体のパスワードを知っている事実が立証されていれば足りる」との姿勢を示した判例と位置づける他の論稿として、Uresk, *supra* note 19, at 622; Gary Kessler and Ann Phillips, Cryptography,

区連邦地方裁判所判決[64]がある。本件は、児童ポルノの所持の被疑事実に関して、捜査機関が請求し、裁判官が発付したデジタルデバイスや外付けハードディスク等への提出命令に対して被疑者が申し立てた救済の可否に関するものである。

FBIは、捜索令状に基づく被告人のデジタルデバイスや周辺機器の捜索により発見された12点のデジタルデバイスの中に、児童ポルノを含むものがありうると判断したが、そのうちの数台は暗号化されており、中身にアクセスできなかった。そこで、スマートフォン、ノートパソコン、外付けハードディスクの３つの解読を被告人に強制する命令を裁判所に請求した。被告人は、スマートフォンとノートパソコンの所有権を認め、パスワードを提供したが、そのパスワードはロック画面を解除するためのものにすぎず、ハードディスクの一部は復号できなかった。ハードディスクは、ノートパソコンと同じ机から押収されたもので、被告人は、押収されたのと同じ内容のハードディスクの所有と、押収されたものと同じ暗号化ソフトを使ってハードディスクを暗号化したことを認める供述をしていた。裁判所から被告人に３台の端末の復号を命じられた被告人は、連邦地裁に対し、命令からの救済を求める申し立てを行った。

連邦地裁は、まず、被告人がデバイスの復号に応じれば、自身がデバイスの解読能力を有している事実を暗示するとし、提出行為の「供述的」性質を認めた[65]。そのうえで、本件のように、捜査機関が特定のファイルではなくハードディスクを丸ごと要求するようなケースでは、被告人がその中身に関

Passwords, Privacy, and the Fifth Amendment, 15.2 Journal of Digital Forensics, Security and Law 2, 11（2020）; Michael Price and Zach Simonetti, Defending Device Decryption Cases, July 2019 The Champion 42, 47（2019）; Sacharoff, *supra* note 14, at 235; Laurent Sacharoff, What Am I Really Saying When I Open My Smartphone: A Response to Orin S. Kerr, 97 Tex. L. Rev. Online 63, 64, n.5（2018）; Kiok, *supra* note 60, at 70; Dan Terzian, The Fifth Amendment, Encryption, and The Forgotten State Interest, 61 UCLA L. Rev. Discourse 298, 300（2013）.

64）　United States v. Spencer, 2018 WL 1964588（N.D. Cal. 2018）.

65）　*Id.*, at *2.

して知識を有している事実が暗示されるわけではなく[66]、被告人がデバイスを復号する能力を有している事実が明確かつ説得的な証拠によりあらかじめ証明されていれば、「自明の帰結」法理を適用できるとした[67]。

結論として、連邦地裁は、３つのデバイスが被告人の住居で発見された点、被告人が、スマートフォンとノートパソコンの所有を認めたうえで、それらのパスワードを提供している点、被告人が、押収されたのと同じ内容のハードディスクを所有しており、暗号化ソフトを使ってハードディスクを暗号化したことを認めている点を根拠に、被告人が３つのデバイスを復号する能力を有している事実は「自明の帰結」であるとして、本件提出行為の強制は修正５条に違反しないとした。

⑵　2011年合衆国第11巡回区控訴裁判所大陪審文書提出命令審　次に、「自明の帰結」法理の適用に際して、「②当局がデバイスの内容に関する知識を有している事実を立証することまで求められる」との姿勢を示した代表的[68]な判例として、2011年合衆国第11巡回区控訴裁判所大陪審文書提出命令審[69]がある。本件は、児童ポルノを共有した被疑事実に関して、捜査機関が請求したハードディスクへの文書提出命令に従わなかった被告人に言い渡された法廷侮辱の制裁の是非が争われた事件の控訴審である。FBI の捜査官が、捜索令状に基づき、被告人が滞在していたホテルの部屋に対する捜索を行ったところ、ノートパソコン２台と外付けハードディスク５台が発見された。科学捜査官による分析の結果、ハードディスクの一部にアクセスで

66）　*Id.*, at *3.

67）　*Id.*

68）　Kerr, *supra* note 54, at 769, n.7. 本判決を「自明の帰結」法理の適用にあたり「当局がデバイスの内容に関する知識を有している事実を立証することまで求められる」との姿勢を示した例と位置づける他の論稿として、Uresk, *supra* note 19, at 627, n. 221; Sacharoff, *supra* note 63, at 64, n.5; Dan Terzian, The Micro-Hornbook on the Fifth Amendment and Encryption, 104 Geo. LJ Online 168, 173（2015）; Vivek Mohan and John Willasenor, Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era, 15 U. Pa. J. Const. L. Height. Scrutiny 11, 19（2012）.

69）　*In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335（11th Cir. 2012）. 本判決に関する邦語文献として、湯淺墾道「判批」情報セキュリティ総合科学８号（2016）36頁以下。

きない領域が見つかった。

そこで、被告人に対して、大陪審に出廷し、ハードディスクの「暗号化されていない中身」を提出するよう求める召喚状が発付された。被告人は、フロリダ州北部地区の連邦検事に対し、出廷の際には修正５条の自己負罪拒否特権を行使し、召喚には応じないと伝えた。司法長官は、被告人の召喚が公益のために必要と判断し、被告人の免責を認めて召喚状に応じる命令を請求する権限を連邦検事に与えた。被告人の出廷を受けて、連邦検事は、フロリダ州北部地区連邦地裁に対し、ハードディスクの「暗号化されていない中身の提出という（被告人の）行為の利用」に限定して同人に免責を認めるように要請した。つまり、免責は、デバイスの提出自体には及ぶものの、その中身には及ばないことになる。連邦地裁がこの要請を認めて命令を発したところ、被告人はハードディスクの復号を拒否した。被告人は、ハードディスクの中身の証拠利用は、自身の供述から派生した証拠の使用にあたるため、自己負罪拒否特権を行使すると説明した。また、同人は、ハードディスクを復号することができない旨の説明も行った。連邦地裁は、その説明を排斥して法廷侮辱の制裁を言い渡した。被告人は不服申し立てを行った。

この申立てを受けた第11巡回区控訴裁判所は、ハードディスクを復号して提出する行為は、被告人が、捜査対象のファイルの存在と場所に関する知識を有し、暗号化された領域を所有・管理しており、その領域にアクセスしたりファイルを復号したりすることができる事実を暗示するとして、本件提出行為の「供述的」性質を認めた[70]。さらに、本件提出行為に「自明の結論」法理が適用されるかどうかについては、ハードディスク内のファイルの存在や、暗号化された領域にアクセスする被告人の能力に関する事実の証明を欠くとし[71]、修正５条違反を理由に連邦地裁の判断を破棄した。

70）　*Id.*, at 1346.

71）　*Id.*

2　パスワードによるデバイスのロック解除を巡る議論

（1）議論の大勢　パスワードの提供や、パスワードがなければ復号することができないデバイスの復号に「供述的」性質が認められるかどうかについては、「供述的」性質を肯定し、修正５条の適用を認める見解が支配的である[72]。この見解が「供述的」性質を肯定する根拠は、①パスワードの入力で「自分はパスワードを知っている」との事実が暗示される点[73]、②パスワード自体を提出させる場合も、それを提出することでパスワードの組み合わせを伝えることになる点[74]、③「復号」は、解読不能な文字列を読解可能なものに変換するという意味で「翻訳」に近く、「コミュニケーション的」である点[75] に求められている。

他方、パスワードの提出やデバイスの復号により暗示される事実に「自明の帰結」法理を適用するにあたっては、第１に、障壁を低くするべきと説く立場、すなわち「被疑者がパスワードを知っている」ことの証明で足りるとする立場と、第２に、高い障壁を課すべきと説く立場、すなわち「被疑者がパスワードを知っている」事実を超える内容の証明を求める立場のものに分かれている[76]。

（2）カー対サシャロフ論争　この２つの立場を巡り、合衆国憲法修正４条および刑事訴訟法研究の第一人者として知られ、前者の立場の代表的な論

72）　数少ない否定例として、Kessler and Phillips, *supra* note 63, at 8. デバイスの所有者以外の人間がパスワードを知っている場合は少なくないため、パスワードを知っているという事実自体は負罪的ではないと説く。

73）　Uresk, *supra* note 19, at 621; Wareham, *supra* note 59, at 65. 論者は、パスワードの入力にはそれを思い出すという「思考」が介在する点も指摘する。

74）　Terzian, *supra* note 68, at 169–170. ただし、パスワードが物理的に記載された記録などが存在する場合は別論であると指摘する。

75）　Price and Simonetti, *supra* note 63, at 43; Stephen Wicker, Forced Decryption and the Fifth Amendment: A Technical Perspective, 106.1 Proceedings of the IEEE 3, 6（2017）. もっとも、Terzian, *supra* note 68, at 171–172は、金庫の鍵を提出するにあたっても、「鍵をどこに置いたか」を思い出す際には思考を働かせることが必要になることに照らし、復号されたデバイスの提出を強制することは「内心」の利用には当たらないと説く。

76）　Kerr, *supra* note 54, at 769, n.9.

者であるオリン・カーと、同じく修正４条やコンピュータ法分野の研究を専門とし、後者の代表的な論者であるローレント・サシャロフ[77]が、互いの論稿を通じて議論を戦わせている。ここでは、両者の議論の整理を通じて、２つの立場の基本的な対立状況を把握する。

前者の立場を代表するカーは、捜査対象者が「パスワードを知っている」事実を当局があらかじめ証明しておけば、パスワードの提供を強制することについては「自明の帰結」法理を適用することができると説く[78]。カーは、その根拠を、パスワードの提供から暗示される供述が「私はパスワードを知っている」事実にすぎない点に求めている[79]。すなわち、捜査対象者が誰かのデバイスを借り、その際にパスワードを教えてもらう例を挙げ、この場合、捜査対象者は、パスワードを知っているが中身については知らないため、「パスワードを知っている」事実を超える内容の供述が暗示されることはないというのである[80]。

カーの見解の背景には、暗号化技術の社会的特性に照らしても、なお修正５条の従来的な理論は妥当することと、暗号化技術の普及で、修正４条のもとで捜索が認められるデータが修正５条により不適切に覆い隠されてしまうことへの懸念がある[81]。

これに対して、サシャロフは、①当局が、被疑者がデータを所有していることをあらかじめ認識しており、②その存在を「合理的な具体性」をもって証明できる場合に限り、そのデータ「のみ」の復号の強制が許容されるべき

77）　ローレント・サシャロフは、2022年現在はデンバー大学ステュルム・ロースクールの教授を務め、主に修正４条やコンピュータ法分野の研究に取り組んでいる。サシャロフは、以下の論稿を通じて前記のオリン・カー教授とパスワードの提供やパスワードでロックされたデバイスの復号への「自明の帰結」法理の適用を巡り論争を戦わせている。See, Sacharoff, *supra* note 14; Sacharoff, *supra* note 63.

78）　Kerr, *supra* note 54, at 769–770, 778, 782–783, 799.

79）　*Id.*, at 769–770.

80）　*Id.*, at 779.

81）　Kerr, *supra* note 54, at 790. See also, Dan Terzian, Forced Decryption as a Foregone Conclusion, 6 Calif. L. Rev. Circuit 27, 34–35 (2015); Terzian, *supra* note 63, at 300.

であると説き[82]、「自明の帰結」法理を、捜査対象の文書ではなくパスワードに適用するのは誤りであると指摘する[83]。サシャロフは、その根拠を、パスワードが提出されれば、単にそれを知っている事実を超えて「復号された文書が存在し、それを被疑者が所有しており、かつそれが真正であることを知っている」という事実が伝わることになる点に求める[84]。

サシャロフの見解の背景には、不合理な捜索押収を禁止する合衆国憲法修正４条と、自己負罪拒否特権を保障する修正５条の双方の背後にある価値観に立ち返り、両条の忌避する網羅的探索がデジタルデバイスに対して行われることを防ぎつつ、後者に関する「自明の帰結」法理の範囲でデータの押収を認めることを通じて、捜査対象者の権利と法執行の利益との調和を図ろうとする趣旨がある[85]。

以上の見解に基づき、サシャロフは、自身に向けられたカーからの「パスワードを提供する行為から暗示される供述は『パスワードを知っている』事実にすぎない」との批判に対して、パスワードを解除する行為は、「デバイスが『おそらく』その人に帰属し」、「同人が『おそらく』そのデバイスの中のファイルを意識的に所有している」事実を伝えることになると反論する[86]。この反論に対してカーは、提出行為により暗示される供述とは、「人がその行為を完結するために何を考えていたのか」を指し、したがって、提出行為の「供述的」性質を検討するうえでは、その行為が「必然的」に明らかにする「内心の状態」を問うべきであると説き、サシャロフの見解には、提出行為に内在する暗黙の供述の有無の判断と、合理性の有無を問題にする

82）　Sacharoff, *supra* note 14, at 208, 251. See also, Minerva Pinto, The Future of the Foregone Conclusion Doctrine and Compelled Decryption in the Age of Cloud Computing, 25 Temp. Pol. & Civ. Rts. L. Rev. 223, 241 (2016).

83）　Sacharoff, *supra* note 14, at 209.

84）　*Id.*, at 235-236.

85）　*Id.*, at 208, 243, 251. 論者は、ここでの網羅的探索を、当局がデバイス内を「自由に歩き回る」と表現する。

86）　Sacharoff, *supra* note 63, at 67.

証拠評価との混同があるとの再反論を加えている[87]。

Ⅳ　生体認証によるデバイスのロック解除と自己負罪拒否特権

捜査機関が、被疑者に対し、指紋や顔認証等の生体認証の解除を強制することが、合衆国憲法修正５条の保障する自己負罪拒否特権に照らして許されるのかどうかを巡っては、それを解除する行為に「供述的」性質が認められるかどうかで見解が分かれている。この点についても、2022年11月現在、合衆国最高裁による判断は示されていないが、令状審査を含めた連邦の下級審や州裁判所では、生体情報を身体的特徴と捉えて「供述的」性質を否定するものが支配的との評価が一般的である[88]。その一方で、前記の2014年ライリー・ケース合衆国最高裁判決等を意識したと見られる、生体認証に修正５条の適用を認めたものも存在する。以下では、生体認証への修正５条の適用に関する判例を概観したうえで、生体認証によるロック解除と自己負罪拒否特権を巡る議論を整理する。

1　修正５条の適用を否定した判例

(1) 2014年バウスト・ケースバージニア州控訴裁判所判決　州レベルにおいて生体認証への修正５条の適用を否定した判例として、2014年バウスト・ケースバージニア州控訴裁判所判決[89]がある。本件は、被告人が、自宅の寝室で被害者に暴行を加えた罪に問われた事件に関するものである。被害者の供述によると、被告人は、暴行現場となった寝室にビデオカメラを設置して常時録画しており、以前には、自身と被害者との性行為の様子が撮影された映像を被害者にメールで送った事実があることに加え、ビデオが被告

87）　Kerr, *supra* note 54, at 780, n.63.

88）　Reitinger, *supra* note 60, at 63; Parikh, *supra* note 60, at 82, 87–88; Cohen and Park, *supra* note 60, at 194; Taylor Ichinose, The Fifth Amendment's Pressing Issue in the Digital Era; Protecting Your Password but What about Your Prints, 57 U. Louisville L. Rev. 353, 372 (2018).

89）　Commonwealth v. Baust, 2014 WL 10355635 (Va. Cir. 2014).

人のスマートフォンに録画記録を送信している事実が認められるとされる。被害者の供述に基づき発付された捜索令状に基づき、警察は、被告人が所有する携帯デバイス、複数の録音機器、各種ディスク、フラッシュドライブ、コンピュータ機器を押収した。もっとも、携帯電話は、パスワードか指紋によるロックが施されていた。そこで、当局は、携帯電話のロックを解除するために、被告人に対して、パスワードまたは生体情報の提出を強制する命令を請求した。

弁護人は、パスワード、指紋の提供のいずれかにより、当局が、被告人の電話の中のすべての記録またはアイテムにアクセス可能になる点で、いずれの提供も「供述的」であると主張した。バージニア州控訴裁判所は、合衆国最高裁における身体的特徴の開示や文書提出と「供述」該当性に関する先例を踏襲し、パスワードの提出行為の「供述」該当性を認めつつ、指紋の提供行為については、その「供述的」性質を否定した[90]。

⑵　2017年イリノイ州東部地区連邦地方裁判所捜索押収令状審　連邦レベルにおいて生体認証への修正５条の適用を否定した判例として、2017年イリノイ州東部地区連邦地方裁判所捜索押収令状審[91]がある。本件は、児童ポルノの受領および所持の被疑事実について、捜査機関が行った捜索押収令状の請求に関するものである。当局は、前記被疑事実の捜査のために、捜索対象の住居に住む４人に対し、自宅で発見される可能性のあるスマートデバイスに指を押させるための押収権限を求めた。裁判所は、指紋による生体認証の解除の強制は合衆国憲法修正５条に違反すると判断し、指紋の押収に関する請求を却下した。当局は、イリノイ州東部地区連邦地方裁判所に審査を求めた。

イリノイ州東部地区連邦地方裁判所は、まず、身体的特徴の開示には「供述的」性質が認められないことを確認した[92]。そのうえで、後記の2017年ダ

90）　*Id.*, at *2, *4. ただし、パスワードの提出に関して「自明の帰結」といえる立証が果たされていなかったとして、被告人の主張を一部認めた。

91）　*In re* Search Warrant Application, 279 F. Supp. 3d 800 (N.D. Ill. 2017).

92）　*Id.*, at 803.

イアモンド・ケースミネソタ州控訴裁判所判決、前記の2014年バウスト・ケースバージニア州控訴裁判所判決を引用し、身体的特徴に関する合衆国最高裁の先例は、生体認証を解除するために指紋の提供を強制する場面にも妥当するとしつつ[93]、生体認証は、対象者が眠っていても行うことができる点に付言し[94]、当局の請求を認めた。

⑶　2018年ダイアモンド・ケースミネソタ州最高裁判所判決　さらには、2018年ダイアモンド・ケースミネソタ州最高裁判所判決[95]において、州最高裁でも、同様の方向性を支持する判決が出された。本件は、被告人が、第２級強盗、軽窃盗、第４級器物損壊の罪に問われた事件に関するものである。本件に先立ち、被告人は、この事件とは無関係の未解決事件で逮捕されており、その際、被告人の靴や携帯デバイスを含む所持品が押収されていた。チャスカ市警察は、本件被疑事実の捜査のために、デバイスの中身の捜索を許可する令状を取得し、その捜索を試みたが、デバイスのロックを解除することができなかった。そこで、警察は、デバイスのロックを解除するために、被告人に対して指紋の提供を強制する権限を求め、カーバー郡連邦地方裁判所に申し立てた。連邦地裁は、指紋の提供の強制は修正５条の保障する自己負罪拒否特権に違反しないと判断し、申し立てを認めた。被告人は、指紋の提供を拒んだものの、民事的裁判所侮辱が認定されたのを受け、指紋を提出した。正式事実審理の結果、被告人に対して、前記の罪について有罪評決が下された。これを受けて、被告人は、指紋の提供を強要されたことは修正５条の保障する自己負罪拒否特権を侵害するものである等の理由で控訴した。

控訴審（前記の2017年イリノイ州東部地区連邦地方裁判所捜索押収令状審で引用されていた2017年ダイアモンド・ケースミネソタ州控訴裁判所判決[96]）において、ミネソタ州控訴裁判所は、生体認証の解除のために強制される指紋の提供には、身体的特徴の開示と同様に「供述的」性質が認められ

93）　*Id.*, at 803-804.
94）　*Id.*, at 804.
95）　State v. Diamond, 905 N.W.2d 870 (Minn. 2018).
96）　State v. Diamond, 890 N.W.2d 143 (Ct. App. Minn. 2017).

ないとして、被告人の控訴を棄却した[97]。

被告人の上訴を受けたミネソタ州最高裁は、身体的特徴の開示に関する合衆国最高裁の先例に照らし、携帯電話のロックを解除するために生体情報を取得することは、身体的特徴を収集する「検査」に準ずるものであるとして、指紋を提供する行為の「供述的」性質を否定した[98]。また、指紋の提供により、被告人の内心が明らかになるわけではないと付言し[99]、本件指紋の提供の強制は修正５条に違反しないと結論づけた。

なお、本判決以降も、同様の方向性を支持するものとして、コンピュータ詐欺および関連活動に従事した被疑事実に関する2018年コロンビア地区連邦地方裁判所捜索令状審[100]、秘密の情報提供者をオンラインで脅迫し、証人を威迫した被疑事実に関する2019年バレラ・ケースイリノイ州東部地区連邦地方裁判所携帯電話捜索令状審[101]、児童ポルノの所持の被疑事実に関する2019年アイダホ州連邦地方裁判所捜索押収令状審[102]、児童ポルノを構成する、またはそれを含む事物にかかわる特定の活動に関与した被疑事実に関する2020年ケンタッキー州東部地区連邦地方裁判所捜索押収令状審[103]が続いている。

2　修正５条の適用を肯定した判例

（1）2017年合衆国イリノイ州東部地区連邦地方裁判所捜索令状審　生体認証への修正５条の適用を肯定した連邦地裁の判例として、2017年合衆国イリノイ州東部地区連邦地方裁判所捜索令状審[104]がある。本件は、対象施

97）　*Id.*, at 150-151.

98）　*Id.*, at 875-876.

99）　*Id.*, at 876.

100）　*In re* Search of［Redacted］D.C., 317 F. Supp. 3d 523（D.D.C. 2018）.

101）　*In re* Search Warrant Application for the Cellular Telephone in United States v. Anthony Barrera, No. 19 CR 439, 2019 WL 6253812（N.D. Ill. Nov. 22, 2019）.

102）　*In re* Search of a White Google Pixel 3XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785（D. Idaho 2019）.

103）　*In re* Search Warrant No. 5165, F.Supp.3d 715（E.D.Ky. 2020）.

104）　*In re* Application for a Search Warrant, 236 F. Supp. 3d 1066（N.D. Ill. 2017）.

設のインターネットサービスを利用した児童ポルノの受信、売買の被疑事実について、捜査機関が捜査のために行った捜索押収令状請求に関するものである。連邦当局は、対象施設内のデジタルデバイスの押収、フォレンジック調査を実施する権限に加え、対象デバイスの中身にアクセスするために、捜査対象者に対して指紋の提供を強制する権限を要求した。

イリノイ州東部地区連邦地方裁判所は、結論として、被疑者が、禁制品が保存されている可能性のあるデジタルデバイスの生体認証を解除するために指紋を提供する行為は、生体認証機能を介して、自身と当該禁制品との結びつきを示す点、ロックを解除することで、デバイスのコンテンツを生産することになる点、認証を解除することで、少なくとも指紋認証機能を設定するためにデバイスにアクセスしたことがあり、現にデバイスとコンテンツの所有・管理に深くかかわっている事実を暗示することになる点を指摘し、本件指紋の提供の「供述的」性質を認めた[105]。その際、人物特定のための指紋の開示が問題とされた前記の1967年ウェイド・ケース合衆国最高裁判決をあげ、同判決は、携帯電話が存在しなかった時代に、指紋押捺を人物特定の目的のみに利用するという文脈で下されたものであり、指紋を使って個人の最もプライベートな情報のデータベースにアクセスする場合とは場面が全く異なると指摘した[106]。さらに、ライリー・ケース合衆国最高裁判決で提起されたプライバシーの社会的懸念に言及し、この懸念は修正５条にも当てはまるとしたうえで、人物特定のための指紋採取の場面と、個人の生活に関する最も詳細な情報を含み、かつ禁制品に直接アクセスできる可能性のあるデジタルデバイスにアクセスするために指紋を採取する場面を同一視することは安直な推論であると断じ[107]、当局の請求を斥けた[108]。

105）　*Id.*, at 1073.

106）　*Id.* ここで裁判所は、前記の2014年ライリー・ケース合衆国最高裁判決を引用し、携帯電話の誕生と普及が1967年当時には予想されえなかったことと、携帯電話という名称はミスリードであり、実際には電話としても使用できるミニコンピュータであることを強調している。

107）　*Id.*, at 1073-1074.

108）　なお、裁判所は、指紋によるロック解除に「自明の帰結」法理が適用される可能性を認めつつ、本件ではその適用に至る立証が果たされていなかったことを示唆している。*Id.*, at 1074.

⑵　2017年イリノイ州東部地区連邦地方裁判所一戸建て住居等への捜索令状審　同様の判断は、2017年イリノイ州東部地区連邦地方裁判所一戸建て住居等への捜索令状審[109]でも下されている。本件は、児童ポルノの受領・所持の被疑事実について、捜査機関が捜査のために行った捜索押収令状の請求に関するものである。本件請求において、FBIは、対象場所やそこに所在する物品に対する捜索押収に加え、物品に含まれうるデジタルデバイスに対するフォレンジック調査を行う権限と、対象場所に在住する４人の家族（同一の姓をもつ夫婦と成人した２人の息子）の指を使用し、デバイスの生体認証の解除を強制する権限を要求した。

イリノイ州東部地区連邦地方裁判所は、対象者が生体認証を解除することで、デバイスとその中に保存されている禁制品を自身が管理・所有していた事実を暗示し、コンテンツを当局に提供することになるとし、生体認証の解除の「供述的」性質を認めた[110]。そのうえで、前記の2014年ライリー・ケース合衆国最高裁判決が、過去に類型化された規範を新技術の文脈に、その合理性を問い直すことなく機械的に適用することに警鐘を鳴らしたものと捉え[111]、個人の指一本でデジタルデバイスに保存される膨大な情報にアクセス可能になったデジタル時代の状況を踏まえて、生体認証の「供述的」性質を確認し、当局の請求を斥けた[112]。

⑶　2018年セオ・ケースインディアナ州控訴裁判所判決　州レベルにおいて生体認証への修正５条の適用を否定した判例として、2018年セオ・ケ

109）　*In the Matter of* Single-family Home & Attached Garage, No. 17 M 18, 2017 WL 4563870（N.D. Ill. Feb. 21, 2017）.

110）　*Id.*, at *1.

111）　*Id.*, at *6.

112）　*Id.*, at *7. なお、同頁では、生体認証への修正５条の適用を主張するKara Goldman, Biometric Passwords and the Privilege Against Self-Incrimination, 33 Cardozo Arts & Ent. LJ 211（2015）を引用し、これを「適切に論じた」と評したうえで、生体認証によるロック解除が暗示する供述が「自明の帰結」であるか、免責対象とされない限り、その解除の強制は修正５条に違反すると結論づけている。なお、同論文の筆者であるカラ・ゴールドマンは、論文公刊当時、ベンジャミン・N・カードウゾウ法科大学院の博士候補生であり、「CARDOZO ARTS & ENT. L.J.」33号の編集委員を務めていた。

ースインディアナ州控訴裁判所判決[113]がある。本件は、被告人が、重罪のストーカー行為、軽罪の脅迫、軽罪の窃盗、軽罪のハラスメント、接近禁止命令に違反する13件の軽罪のプライバシー侵害の罪に問われた事件について、その手続の過程で被告人に法廷侮辱が認定されたことの是非に関するものである。当初、被害者からのレイプ被害を訴えていた被告人は、捜査の過程で、HCSD（ハミルトン郡保安官事務所）によるスマートフォンの中身の「フォレンジックダウンロード（forensic download）」に同意してスマートフォンを提出し、その返却を受けていた。中身の確認後、郡保安官事務所は、被告人による被害者に対する前記被疑事実の捜査に切り替え、スマートフォンのデータと被害者の供述に基づき、被告人を、重罪のストーカー行為等の容疑で逮捕・訴追した。後日、接近禁止命令違反を理由に、13件の軽罪のプライバシー侵害の罪で新たに訴追した。

郡保安官事務所は、被告人のスマートフォンに対する捜索令状を得た。令状は、スマートフォンのロックを生体認証やパスワード、その他の方法で強制的に解除でき、被告人が命令に従わない場合には裁判所侮辱の対象となる旨が記載されていた。被告人から命令に従う意思がない旨の通知を受け、郡保安官事務所は、被告人が命令に従わないことに正当な理由を問う審査をハミルトン郡高等裁判所に申し立てた。審理の結果、裁判所は、法廷侮辱を認定し、被告人に対して、ロックの解除または刑務所への収監を命じた。被告人は、控訴に伴う法廷侮辱の制裁の停止を申請したうえで、インディアナ州控訴裁判所に控訴した。

控訴裁判所は、まず、前記の2014年ライリー・ケースや2018年カーペンター・ケース合衆国最高裁判決等を引用し、修正５条の自己負罪拒否特権は、合衆国の基本原則を反映したものであり、技術の進歩により変更されてはならないどころか、テクノロジーの移り変わりを認識し、一貫して適用されなければならないと述べ[114]、修正５条についても、両判決で示された姿勢を

113）　Seo（n.62）.

114）　*Id.*, at 436-437.

踏襲することを明らかにした。そのうえで、ロック解除に伴うデバイスの中身の「復号」に着目し、デバイスの「復号」は、当局が解読を欲する判読不能なファイルをその求めに応じて再生するものであり、単なる文書の提出よりも「供述的」な性質が強いと指摘した[115]。また、金庫の「鍵」と壁掛け金庫の「番号」のアナロジーをスマートフォンに当てはめる比喩には無理があり、最も秘匿性の高い性質を持つアイテムを含む文字通りの「金庫」や、「第２の脳」、「内心の延長」といった比喩を用いるのが適切であると説き、修正５条違反を理由に被告人に対する法廷侮辱の認定を取り消した[116]。

（4）2019年カリフォルニア州北部地区連邦地方裁判所オークランドの住宅捜索令状審　さらに、パスワードと生体認証の機能的な同一性に加え、両者の一体性に言及して生体認証への修正５条の適用を肯定した連邦地裁の判例として、2019年カリフォルニア州北部地区連邦地方裁判所オークランドの住宅捜索令状審[117]がある。本件は、恐喝の被疑事実について、捜査機関が捜査のために行った捜索押収令状の請求に関するものである。SNS を通じた脅迫の嫌疑で、連邦当局は、カリフォルニア州オークランドの対象住宅に所在するデジタルデバイスを含む物品の捜索押収と、デバイスの生体認証を解除するために、捜索時に居合わせた個人に、指紋や顔、虹彩認証等の生体認証機能を使用するよう強制できる権限を請求した。

カリフォルニア州北部地区連邦地方裁判所は、まず、生体認証とパスワードが、機能的には同一の役割を果たす点と、生体認証に失敗した場合にパスワードが要求される場合があり、両者に一体性が認められる点に言及し、デバイスロックの場面での生体情報の提供と、人物特定のための身体的特徴の開示を同列にはできないと指摘した[118]。そのうえで、被疑者が生体認証を解除する行為は、デバイスが自身の所有・管理下にあった事実を暗示し、自

115）　*Id.*, at 438.
116）　ただし、後に最高裁で破棄された。
117）　*In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010（N.D. Cal. 2019）.
118）　*Id.*, at 1015-1016.

身のアクセス権を認証するものであるとして[119]、修正５条違反を理由に当局の請求を斥けた。

なお、同年に、同じくカリフォルニア州北部地区連邦地裁において、生体認証への修正５条の適用を肯定した判例として、オピオイド鎮痛薬の違法な処方と流通を含む麻薬密売活動を行った被疑事実に関する2019年ウォレント・ケースカリフォルニア州北部地区連邦地方裁判所判決[120]がある。加えて、同様の方向性の判断を示した最近の連邦地裁の判例として、被告人が、児童ポルノの受領および所持の罪に問われた事件に関する2020年ライト・ケースネバダ州連邦地方裁判所判決[121]が続いている。

3　修正５条の適用を巡る議論

(1) 修正５条の適用否定説　生体認証によるロック解除の強制について、合衆国憲法修正５条が保障する自己負罪拒否特権の適用を否定する立場は、その根拠を①生体認証は思考を介在しない点と、②生体情報は指紋や声紋に等しい点に求める。このうち、①については、生体認証機能は対象者の意識がなくても作動することに表れているように、それを解除する行為は「金庫の鍵の明け渡し」に近いため、「供述的」とはいえないと説く[122]。②については、生体認証の解除に伴う生体情報の提供は、先例で修正５条の適用が認められてこなかった指紋や声紋の提供に等しいにもかかわらず、同条を生体情報に及ぼせば、従来の判例法理に反して同条と修正４条との垣根を壊すことになると説く[123]。

119）　*Id.*, 1016.

120）　United States v. Warrant, No. 19-mj-71283-VKD-1, 2019 WL 4047615 (N.D. Cal. Aug. 26, 2019).

121）　United States v. Wright, 431 F. Supp. 3d 1175 (D. Nev. 2020). 同判決は、前記の2019年カリフォルニア州北部地区連邦地方裁判所オークランドの住宅捜索令状審を「最も説得力がある」と評している。*Id.*, at 1187.

122）　Nathan Lyon, Compelling Decryption of a Smartphone under the Fifth Amendment, 5 Utah J. Crim. L. 57, 61, 65 (2021); Opher Shweiki and Youli Lee, Compelled Use of Biometric Keys to Unlock a Digital Device: Deciphering Recent Legal Developments, 67 Dep't of Just. J. Fed. L. & Prac. 23, 37 (2019).

123）　Antonio Vayas, Say Cheese: How the Fourth Amendment Fails to Protect Your Face, 51 Seton

（2）修正５条の適用肯定説　もっとも、前記の通り、パスワードについては修正５条の保護が及ぶとの理解が支配的であることを前提にすると、同じく認証機能を果たす生体認証とパスワードとで、修正５条の適用の可否が変わることになる。携帯デバイスのユーザーの視点から言い換えれば、ユーザーが生体認証を選ぶか、パスワードによるロックを選ぶかで、修正５条の保護を得られるかどうかが変わってしまうという「ジレンマ」に陥ることになる[124]。

この「ジレンマ」を背景に、生体認証によるロック解除の強制に修正５条の適用を肯定する見解もみられる。この見解は、生体認証を解除する行為の「供述的」性質を認める見解と、生体認証や携帯デバイスがもつ社会的特性に照らして「供述」概念の拡張やアップデートを求める見解に大別できる。

生体認証を解除する行為の「供述的」性質を認める見解は、生体認証の解除を通じて、解除を行った者がアクセス権者や管理者であるとの事実が暗示されることを理由に、単に人物特定のために身体的特徴を開示する行為と、生体認証を解除する行為を同列に論じるべきではないと説く[125]。ただし、

Hall L. Rev. 1639, 1641, 1665–1667 (2021); Ari Rubin, A Facial Challenge: Facial Recognition Technology and the Carpenter Doctrine, 27 Rich. JL & Tech. 1, 31 (2020); Kerr and Schneier, *supra* note 18, at 1003; John Larkin, Compelled Production of Encrypted Data, 14 Vand. J. Ent. & Tech. L. 253, 270 (2011); Terzian, *supra* note 68, at 169; Mohan and Willasenor, *supra* note 68, at 24. See also, Lyon, *supra* note 122, at 58.

124）　Bryan Choi, The Privilege against Cellphone Incrimination, 97 Tex. L. Rev. Online 73, 76–77 (2018). 論者は、セキュリティ分野では一般により安全性が高いといわれる生体認証が、法律分野においては、生体認証の方が法執行のために利用されやすいという逆転現象が生じていると指摘する。See also, Aaron Chase, Secure the Smartphone, Secure the Future: Biometrics, Boyd, a Warrant Denial and the Fourth and Fifth Amendments,17 Hastings Race & Poverty LJ 577, 600 (2020); Herrera, *supra* note 60, at 780–782; Ichinose, *supra* note 88, at 370–371; Bryan Choi, For Whom the Data Tolls: A Reunified Theory of Fourth and Fifth Amendment Jurisprudence, 37 CARDozo L. REv. 185, 244, 246 (2015).

125）　Redfern, *supra* note 60, at 627; Brittany Carnes, Face ID and Fingerprints: Modernizing Fifth Amendment Protections for Cell Phones, 66 Loy. L. Rev. 183, 204 (2020); Ichinose, *supra* note 88, at 371. See also, Harrison Metz, Your Device Is Disabled: How and Why Compulsion of Biometrics to Unlock Devices Should Be Protected by the Fifth Amendment Privilege, 53 Val. UL Rev. 427, 446–449, 455–457 (2018); Raila Brejt, Abridging the Fifth Amendment: Compelled Decryption, Passwords, & Biometrics, 31 Fordham Intell. Prop. Media & Ent. LJ 1154, 1177, 1197 (2021). これ

この見解に対しては、先例によれば、ある事実の伝達を強制することと、身体的特徴の開示が強制されることに起因して自己に不利益な事実の暗示が生じることとは、基本的に区別されており、生体認証の解除により自身がデバイスの所有者等である事実が伝わるとしても、それ自体は「供述」とはいえないとの異論がある[126]。そこで、生体認証の解除の強制に修正５条の適用を認める立場から、生体認証やデジタルデバイスがもつ社会的特性[127]に照らして「供述」概念の拡張やアップデートを求める見解が示されている。この見解は、①デバイスに保存される中身の量（そこから転化した質[128]）、②生体認証の普及に伴うプライバシーへの懸念、③パスワードとの機能的な同一性、④携帯電話がもつ「内心（あるいは脳や身体）の拡張」としての特質といった点から、「供述」概念の拡張やアップデートを図り、修正５条を生体認証の解除に適用すべきであると説く[129]。

このうち、①（デバイスに保存される中身の量・質）からは、携帯デバイスに保存されるデータの量・質に照らし、当局による携帯電話へのアクセスの態様ではなく、そのアクセスで明らかになる（負罪的な）情報の広範さと、その結果が被疑者の自己負罪拒否特権に及ぼす影響に着目し、「供述」該当性判断において、デバイスの内容がもつ負罪性を考慮すべきであると説かれ

らはいずれも、デバイスの中身について「自明の帰結」といえる程度の証明がなされた場合には修正５条の適用が否定される余地があることを明言する。

126）　Lyon, *supra* note 122, at 611; Erin Sales, The Biometric Revolution: An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination, 69 U. Miami L. Rev. 193, 228–229 (2014).

127）　後述の携帯電話がもつ「内心（あるいは脳や身体）の拡張」としての特質に着目して「供述」概念の生体認証への拡張を求める立場の論者であるアリエル・レッドファーンは、携帯電話がもつ社会的な特質に着目して行う法解釈を「公共政策のレンズ（the lens of public policy）」を通した自由な解釈（liberal interpretation）と称する。Redfern, *supra* note 60, at 613, 622–623, 625–627.

128）　Carnes, *supra* note 125, at 206–208は、512ギガバイトの携帯電話には、フロッピーディスク358,400枚分の情報が保存できることを前提に、「ギガバイト」単位の潜在的に自己負罪的な情報を保存した携帯電話のロック解除を当局が強制できることになれば、弾劾主義を伝統とする刑事司法制度は崩壊すると説く。See also, Casey Coffey, Place Your Finger on the Home Button: The Legality of Compelling Biometrics, 31 U. Fla. JL & Pub. Pol'y 307, 315 (2020).

129）　なお、ここでは、生体認証がもつ社会的な特性に関するそれぞれの観点を並列的に整理しているが、これらは相互に対立・排斥するものではない。

る[130]。②（生体認証の普及に伴うプライバシーへの懸念）からは、修正５条は同４条と相まってプライバシーを保護するとの理解を前提に、修正５条の適用範囲を生体認証に拡張しなければ、その普及に伴い個人のプライバシーへの過干渉や侵入の危険性が高まり、自己負罪拒否特権は没却されることが懸念されている[131]。③（パスワードとの機能的な同一性）からは、パスワードによるロック解除と生体認証によるロック解除は、その解除や復号の方法が異なるにすぎず、機能的に同一であるため、前記の「ジレンマ」に照らして、解除行為自体ではなく、当局側の行動の性質に着目し、当局が、適正な憲法的手続を科学技術で迂回しようとしていないかどうかが問われるべきであるとの指摘がある[132]。④（携帯電話がもつ「内心の拡張」としての特質）からは、個人の携帯デバイスは、いまやその「内心の延長」、自己の「外付けのハードディスク」と把握されるべき時代を迎えており、生体認証機能の普及を通じた自己負罪拒否特権の潜脱を許すべきでないと説かれる[133]。

130）　Carnes, *supra* note 125, at 201, 203. See also, Chase, *supra* note 124, at 590.

131）　Brejt, *supra* note 125, at 1198; Chase, *supra* note 124, at 579, 580; Metz, *supra* note 125, at 428–429, 462–463.

132）　前記の「ジレンマ」を指摘する論稿に加え、以下も参照。Lemus, *supra* note 60, at 561, 555–556; Metz, *supra* note 125, at 454–455; Madeline Leamon, Unlocking the Right Against Self-Incrimination: A Predictive Analysis of 21st Century Fifth Amendment Jurisprudence, 64 Wayne L. Rev. 583, 598- 599（2018）; Ichinose, *supra* note 88, at 374, 383; Goldman, *supra* note 112, at 226–227, 229 234–235. なお、Sales, *supra* note 126, at 227–228は、生体認証の設定の際にはパスワードも設定する必要があり、生体認証による解除は実際にはパスワードで裏づけられている点を捉え、生体認証によるロック解除の「供述」性を強調する。なお、類似の観点として、生体認証とパスワードに共通する「認証」機能がもつ社会的な意味合いに着目するものもある。ここにいう「認証」とは、①一意のものの提示、すなわちユーザー識別子のような、独立した一意の対象を表す属性値の認証サブシステムへの提示を意味する「識別（identification）」と、②一意の識別子の裏づけ、すなわち「プライベートキーで署名された値（value with signed private key）」のように、属性とその属性を主張するものとの結合を証明するための証拠となる認証情報による裏づけを意味する「照合（verification）」の２要素からなるデバイスの使用者の同一性確認のプロセスを指す。Apple 社の “FaceID” でいえば、①設定された顔のスキャンデータという一意の属性値の提示による「識別」、②あらかじめ設定された顔のスキャンデータとの「照合」がそれぞれ対応する。See, Reitinger, *supra* note 60, at 64, 74–75, 80–81.

133）　Choi, *supra* note 124, at 74–75. See also, Chase, *supra* note 124, at 600; Redfern, *supra* note 60, at 613, 622–623, 625–627; Choi, *supra* note 124, at 244. 同旨として、Metz, *supra* note 125, at

以上の①～④といった生体認証や携帯デバイスがもつ社会的特性に照らして「供述」概念の拡張やアップデートを求める見解の背後には、前記のライリー・ケースやカーペンター・ケース合衆国最高裁判決で示唆された、新しい技術と古い法律との衝突という問題に取り組むべきであるとの発想がある[134]。

もっとも、この見解に対しては、生体認証への修正５条の適用を否定する立場から、生体認証とパスワードとの機能的な同一性により「供述的」でないものを「供述的」に転化することはできないとの批判が加えられている[135]。

V　若干の考察

1　パスワードによるデバイスのロック解除を巡る議論からの示唆

すでに見たように、パスワードによるデバイスのロックの解除に関しては、「自明の帰結」法理の適用に際して、当局により、①被疑者が媒体のパスワードを知っている事実が立証されていれば足りるのか、②それを超えて、当局がデバイスの内容に関する知識を有している事実を立証することまで求められるのかを巡り、見解が対立している。

双方の見解を踏まえると、両者のスタンスの違いは、まず「パスワードを

457-458は、携帯電話等を「個人の私生活全体が入ったデバイス」と捉え、そのようなデバイスが想定されていなかった時代の先例の射程を限定すべきと説く。さらに、人の「内心」が計測可能になりつつある現状において、生体情報＝非供述的という区分を維持することに警鐘を鳴らすものとして、Mohan and Willasenor, *supra* note 68, at 26.

134）　生体認証がもつ社会的な特性を考慮する論者のほとんどは、両判決（とくにライリー・ケース合衆国最高裁判決）を引用している。一例として以下を参照。Carnes, *supra* note 125, at 209; Choi, *supra* note 124, at 76-78; Metz, *supra* note 125, 442-443, 455. なお、Choi は、ライリー・ケースおよびカーペンター・ケース合衆国最高裁判決などには、携帯電話やスマートフォンを「他のデジタルデバイス」と同一視することへの不快感が表れているとしたうえで、「内心の拡張」と捉えられるのは携帯電話やスマートフォンなどの個人用携帯デバイスにとどまるとしている。

135）　Shweiki and Lee, *supra* note 122, at 37.

知っている」との事実からいかなる事実が暗示されると解するかにある。①の見解を採る代表的な判例である2018年スペンサー・ケースカリフォルニア州北部地区連邦地方裁判所判決は、被疑者が復号されたデバイスを提出しても、そこから自身の内心が暗示されるわけではないとする。この見解の代表的な論者であるオリン・カーも、たまたまデバイスを借りた者がパスワードを知っている例に依拠し、「自明の結論」法理の適用には、「被疑者がパスワードを知っている」事実の証明で足りるとする。その一方で、②の見解を採る代表的な判例である2011年合衆国第11巡回区控訴裁判所大陪審文書提出命令審や、その代表的な論者であるローレント・サシャロフは、被疑者が復号されたデバイスを提出することで、自身が暗号化された領域を所有･管理し、そこにアクセスしている事実が暗示されるとする。

また、もう１つのスタンスの違いは、「パスワードを知っている」との事実から暗示される事実を認定するにあたり、その蓋然性で足りるか、必然性まで要求されるかにある。このことは、②の見解を採るサシャロフが、①の見解を採るカーに「デバイスが『おそらく』その人に帰属し」、「同人が『おそらく』そのデバイスの中のファイルを意識的に所有している」事実を伝えることになるとの反論を加えたのに対し、カーが、提出行為に内在する暗黙の供述の有無の判断と、合理性の有無を問題にする証拠評価との混同を指摘し、再反論を行ったことに表れている。

たしかに、デバイスのロックを解除できる者がデバイスの所有・管理・アクセス権者であることが一般的である実情に照らせば、②の見解には説得力があるように思われる。もっとも、身体的特徴の開示に関する合衆国最高裁の先例や、文書提出に関する前記のフィッシャー・ケース合衆国最高裁判決のように、修正５条と修正４条を分断的に理解し、開示を強制される情報の中身が自己に不利益に働くかどうかと、提出行為自体に内在する「供述」性の峻別を徹底しようとすれば、①の見解に近接することになる。

このように考えると、両者の見解の相違の根本は、修正５条と修正４条の関係を、フィッシャー・ケース合衆国最高裁判決がそうしたように分断的に

捉えるか、少なくともデジタルデバイスの文脈ではより競合的に捉えるかにあるといえるのではないだろうか。実際、伝統的な「供述」概念に照らし、デバイスに保存されたデータのもつ自己負罪的な側面を厳格に排除しようとするカーとは異なり、修正５条と修正４条の双方の価値の裏づけを網羅的探索への忌避感に求めたサシャロフの見解の背景には、当局によるデバイスの中身に関する知識についての立証があらかじめ要求されなければ、「被疑者がパスワードを知っている」との事実が立証されるだけで、当局がデバイスの中身を「自由に歩き回る」ことができるようになることに向けた危惧があった。果たして、デバイスの中身に対する保護は修正４条で十分と考えるのか、それでは足りず、デバイスの中身に着目して修正５条による保護を重ねるべきなのか。仮に保護が十分でないとすれば、少なくともデジタルデバイスとの関係では、修正５条と修正４条の関係を再考し、パスワードでロックされたデバイスに対する自己負罪拒否特権の保障のあり方を模索する必要があるといえる。

2　生体認証によるデバイスのロック解除を巡る議論からの示唆

⑴　生体認証を解除する行為がもつ「供述」的性質の有無と「ジレンマ」

前述の通り、パスワードによるロックの解除については「供述」性を認める見解が支配的であるのに対して、生体認証によるロック解除に関しては、少なくとも判例の大勢は、身体的特徴の開示に関する合衆国最高裁の先例を踏襲し、生体認証に用いられる指紋・声紋・容貌等の生体情報はあくまで身体的特徴であり、その提供には「コミュニケーション的」側面、すなわち「供述的」性質が認められず、したがって生体認証の解除の強制には修正５条は適用されないとする見解が支配的との評価が一般的である。また、生体認証は、生体情報さえあれば、対象者に意識がなくとも解除することが可能であることも、この見解の説得力を高めている。たしかに、この考え方は、フィッシャー・ケース合衆国最高裁判決が示した、修正５条と修正４条を分断的に理解し、開示を強制される情報の中身が自己に不利益に働くかどうかの問

題と、提出行為自体に内在する「供述」性を厳格に峻別する考え方に照らしても説得的である。金庫の中に被疑者自身に不利益な証拠があるからといって、その「鍵」の押収を禁止する理由はない。生体情報自体に「コミュニケーション的」な側面がなく、したがって金庫の「鍵」のアナロジーが妥当すると考えるならば、この見解の妥当性は高いといえる。

しかし、この見解を採った場合、デバイスのユーザーが、ロックの方法として、同じく認証機能を果たす生体認証とパスワードのどちらを選ぶかにより、修正５条の保護を得られるかどうかが変わってしまうという「ジレンマ」に陥ることになる。さらにいえば、今後、生体認証の普及が進み、パスワードに取って代わるほど、デバイスに対して自己負罪拒否特権を行使できる機会は失われることになる。もっとも、修正５条と修正４条を分断的に捉え、「供述」性の有無の分水嶺を「コミュニケーション的」側面の有無に求める従来の「供述」概念に照らせば、生体情報が身体的特徴にすぎないこと自体は否定しがたい。そこで、前記の「ジレンマ」を解消するには、生体認証や携帯デバイスがもつ社会的特性に照らした「供述」概念のアップデートが求められることになる。しかし、それらの社会的特性は、少なくとも合衆国憲法修正５条や日本国憲法38条１項が制定された時代にはまったく想定されておらず、それぞれの文言にも見出しがたい、両条項の埒外にある純粋に法政策的な要素である。このような法政策的な要素を考慮し、従来の「供述」概念を拡張して、「供述」でないものを「供述」とすることは許されるのか。

(2)　デジタル時代のアメリカ自己負罪拒否特権論が投げかけるもの　だからといって、前記の「ジレンマ」を放置すれば、科学技術の進展につれ、デジタルデバイスが自己負罪拒否特権で保障される機会が奪われる事態は避けられなくなる。この「ジレンマ」は解消されなければならないとするならば、やはり、これまで当然視されてきた、「コミュニケーション的」側面の有無を基準とする「供述」概念を時代に合わせてアップデートするしかないのだろうか。

ここで日本に目を向けてみると、アメリカにおける生体認証や携帯デバイ

スのもつ社会的特性に照らして既存の「供述」概念のアップデートを図る議論は、日本における刑事訴訟法、とりわけ捜査法の「法解釈」を巡る近時の議論と重なる。具体的には、権利義務の内容を確定してその侵害を問題にする従来的な主観法的解釈の限界が指摘され[136]、それに代わり、普遍的な法・価値秩序に照らして主観的権利を割り当てる客観法の思考を、主観法的解釈に取り込みこれを「鍛えなおす」ことを試みる法解釈[137]や、法政策分析を通じた法解釈[138]といったあり方が提唱されている。後者の法政策分析を通じた法解釈は、流動的・動態的な法形成を志向し、法解釈に政策的帰結を反映させようとする点で、「供述」概念のアップデートを図る議論と親和的である[139]。この法政策分析を通じた法解釈のあり方が説かれる背景には、普遍的な「権利」を想定し、その固定的・静態的な内実を追究してきた従来の刑事訴訟法学に広く見られる姿勢への懐疑がある。これをアメリカで見られるパスワードと生体認証との「ジレンマ」に当てはめると、そこには、自己負罪拒否特権に関しても、伝統的な三段論法を前提にした法解釈や権利論の限界、すなわち自己負罪拒否特権の「本質」に立ち返り、大前提としての「供述」の内実を明らかにしたうえで、小前提たる具体的事実としての生体認証によるロック解除行為に適用するという方法論の限界が顕在化することにな

136）　その限界を浮き彫りにした著作として、稲谷龍彦『刑事手続におけるプライバシー保護』（弘文堂、2017）。限界の具体例として、主観法的解釈が依拠する各種「権利」概念が空虚であるため、規範的な判断基準をもたない点や、それゆえに、法的評価が論者の個人的な価値判断に流されやすく、検証可能性や共有可能性に乏しい点、ひいては、流動し価値観が多様化する社会に対応することが困難な点をあげることができる。

137）　笹倉宏紀「強制・任意・プライヴァシー」酒巻匡＝大澤裕＝川出敏裕編『井上正仁先生古稀祝賀論文集』（有斐閣、2019）253頁以下。

138）　稲谷龍彦「刑事訴訟法解釈の方法」山本敬三＝中川丈久編『法解釈の方法論』（有斐閣、2021）255頁以下。論者は、法政策分析が、立法論のみならず、「これからの刑事訴訟法解釈」にとって必要不可欠であると説く。

139）　ただし、稲谷のいう法政策分析を通じた法解釈の視点からパスワードと生体認証の「ジレンマ」の問題を眺めた場合に、合衆国最高裁が「供述」該当性の判断基準を「コミュニケーション的」側面の有無に求めてきたことが、裁判所の踏み込んだ憲法解釈による権利内容の固定化と受け止められるのか、「供述」概念のアップデートを図り生体認証の解除を「供述」と解することが、裁判所のもつ制度的能力の逸脱とみなされることになるのかには、留意を要する。

るのだろうか。そうであるとすれば、社会のデジタル化が進む中で、捜査法、ひいては刑事訴訟法とその解釈のあり方を抜本的に見直すべき時期が来ているのかもしれない。

もっとも、法政策分析を通じた法解釈に対しては、個人の尊厳に根差した人権概念を、利益衡量の中に埋没させることにつながるのではないかとの危惧も指摘されている[140]。たしかに、アメリカにおいて、生体認証や携帯デバイスの社会的特性に照らした「供述」概念のアップデートを説く論者らは、自己負罪拒否特権の保障範囲を拡張する方向で議論を展開しているが、捜査法の目的に照らして合理的でない権利の「権利性」を否定する方向に作用する可能性も否定できない。その一方で、利益衡量の中に人間の尊厳が埋没されてしまう懸念は、主観法的解釈を採った場合にも妥当し、主観法的解釈を採るかどうかにかかわらず、利益衡量により埋没されるべきではないものや価値の内実を明確にすることこそが重要であるとの指摘もある[141]。

ここで改めて考えてみると、そもそも、なぜ自己負罪拒否特権は「供述」のみを保護するのか。その実質的根拠は今なお必ずしも明らかではない[142]。その根拠が十分に明らかでないにもかかわらず、「供述」の文言に固執し、修正５条と修正４条を分断したことや、その理解に基づき、「供述」的性質の有無を分ける基準を「コミュニケーション的」側面に求めた正当性は、十分に説明されているといえるだろうか。また、両条項の分断的な理解や「コミュニケーション的」側面という基準自体に一定の合理性が認められるとしても、その基準は、あくまでそれが採用された当時の時代状況を背景にした１つの基準であり、「供述」概念の内実ではなかったのではないか[143]。仮に、

140）　後藤昭「捜査の法的規制」川崎英明＝後藤昭＝白取祐司編著『刑事司法改革の現段階』（日本評論社、2021）90頁以下、97-98頁。

141）　緑大輔『刑事捜査法の研究』（日本評論社、2022）391頁。稲谷・前掲注（138）261頁および注（16）も参照。

142）　ドイツにおける呼気検査制度をめぐる議論を素材に、憲法38条１項の保護対象を「供述」の文理に限定する必然性はないと説く近時の邦語文献として、松倉治代「憲法38条１項の保護対象は『供述』に限られるか」立命館法学375=376号（2018）396頁以下、418頁。

143）　暗号化や認証技術の存在を前提とする今日における「コミュニケーション的」側面の有無

このように考える余地があるのだとすれば、今求められるのは、自己負罪拒否特権と令状主義双方の「本質」に立ち返り、「供述」概念の内実に迫る試みであるといえるかもしれない。

今後、いずれの方向に進むにせよ、デバイスのロック解除の強制を巡るデジタル時代のアメリカ自己負罪拒否特権論は、憲法条項を含む刑事訴訟法の法解釈のあり方や、自己負罪拒否特権と令状主義の関係、その背後にある両概念の「本質」といった、刑事訴訟法（学）の根本を激しく揺さぶる問題であるといえる。

Ⅵ　むすびにかえて

本稿では、パスワードと生体認証との間で生じる「ジレンマ」が、デジタルデバイスと自己負罪拒否特権という各論的なテーマを超え、不合理な捜索押収を禁止する修正４条やその背後にあるプライバシーと自己負罪拒否特権の関係という、同特権や令状主義の「本質」を揺さぶる問題であることを示した。反面で、そのような「本質」に拘泥し、「供述」概念の内実とそこからの演繹に固執してきた姿勢こそが、デジタル時代において自己負罪拒否特権を危機にさらしているとも受け取れる。その意味で、デジタルデバイスがもつ社会的特性に照らして「供述」概念のアップデートを図る議論や、法政策分析を通じた法解釈は、非常に魅力的である。

しかし、それでもなお、以下の２点の理由から、自己負罪拒否特権の内実を模索する作業に着手する意義は小さくないように思われる。第１に、そもそも前記の「ジレンマ」は、デジタル時代の到来がきっかけで浮き彫りになったにすぎず、その根本的な原因は、自己負罪拒否特権に関する先例や通説の側の誤解、歴史的背景を異にする基準への過度な固執にある可能性がある。第２に、たとえ誤解ではなかったとしても、捜査法の文脈ですでに指摘され

による従来の二分論の適合性に疑問を呈する邦語文献として、湯淺・前掲注（69）48頁。

ている、主観法的解釈のもとで形成されてきた理論を捨て去ることへの躊躇や、法律専門家の法的知性への働きかけやすさとった利点等は、自己負罪拒否特権を巡る議論にも当てはまる[144]。

近時、日本においても、デジタルデバイスの暗号解除に関わる制度設計の検討が求められている現状を指摘する論稿[145]や、制度化に際して自己負罪拒否特権との抵触を避けるために求められる具体的な要素を提示する論稿[146]がみられる。これまで、アメリカと同様に「供述」該当性判断の基準を「コミュニケーション的」側面の有無に求める見解が一般的であった日本の状況に照らせば、今後、制度化が進み、日本でもパスワードと生体認証との「ジレンマ」が生じる日が来る可能性は否定できない。そのことを念頭に、法政策分析を通じた刑事訴訟法解釈がこれから求められていく可能性と、その方向性のもとで展開される議論の動向にも目配りしつつ、自己負罪拒否特権と令状主義の関係、その背後にある両概念の内実を探究し、デジタル時代におけるデバイスの保護を中心に、ひいては犯罪捜査全般に対する規律のあり方を検討する機会をもちたい。

144）　笹倉・前掲注（137）。
145）　丸橋「黙秘権」・前掲注（16）173頁。
146）　山田「２・完」・前掲注（16）302頁。